FINAL REPORT

Assessment Briefs

FORGING NEW COALITIONS

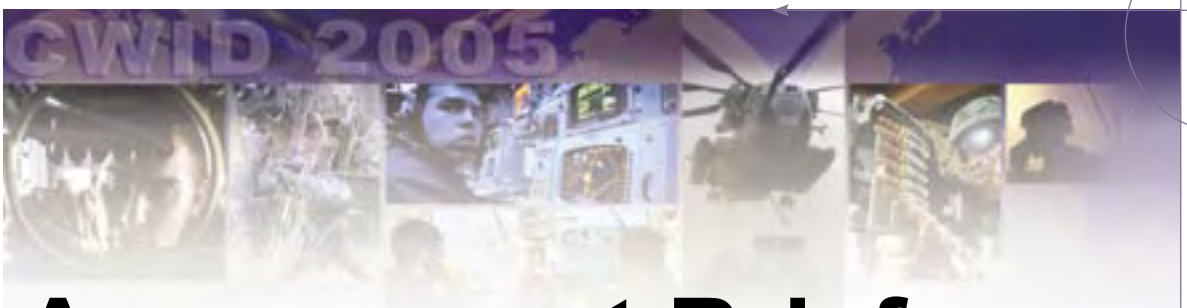
This Assessment Briefs booklet and the unabridged CWID 2005 Final Report are on the CD in interactive form, designed to open in your browser and Adobe Acrobat Reader. Insert the CD into your CD drive. An autorun file will open automatically.

If you have autorun capability disabled, open the CD through MY COMPUTER on a Windows System or click on the CD icon. Then click on the file named START_HERE.

Published February 2006

Coalition Warrior Interoperability Demonstration Joint Management Office, Hampton, Va.

www.cwid.js.mil



Assessment Briefs Booklet Contents

* Unabridged report available for download at www.cwid.js.mil

NOTES

INTRODUCTION

Executive Summary

The Coalition Warrior Interoperability Demonstration (CWID) is an annual Chairman of Joint Chiefs of Staff event with the international community to investigate command and control, communications, computers, intelligence, surveillance and reconnaissance solutions to near-term coalition challenges. The name of the program was changed from Joint Warrior Interoperability Demonstration (JWID) to CWID to better describe the larger community of participants, including national and international governmental agencies. This year's event built on the previous year's demonstration with agencies outside of the Department of Defense (DoD) in the area of Homeland Security (HLS) and Homeland Defense (HLD).

- CWID 2005 provided opportunity for information sharing and investigation of interoperability solutions among many disparate entities, including HLS and HLD partners. U.S. Northern Command (USNORTHCOM) was the Host Combatant Commander for 2004 and 2005. To investigate HLS/HLD solutions, USNORTHCOM invited the Defense Threat Reduction Agency (DTRA), Federal Emergency Management Agency (FEMA), the U.S. Coast Guard and the National Guard Bureau to participate. The international community, participating in the traditional military operations scenario, consisted of Australia, Canada, New Zealand, United Kingdom, Republic of South Korea, NATO and NATO-invited Partnership-for-Peace nations.

- This year 48 U.S. Interoperability Trials (IT) participated in the two-week CWID execution period. During the CWID planning cycle, trials, their sponsors and the CWID Joint Management Office support staff created a Master Scenario Events List (MSEL) containing more than 2,700 events used to execute the CWID 2005 scenario. Over 400 operators from the military and supporting agencies, at multiple U.S. and coalition sites, executed the MSELs, evaluating and reporting on trial performance.

- The CWID 2005 Execution results were noteworthy in that most ITs successfully achieved their stated objectives. The IT assessment summary contained in this booklet and in the companion Compact Disk located on the inside front cover, clearly detail the performance and assessment of each technology demonstration. Of particular note are those ITs which continue development actions described in the "CWID 2005 Successes" section located on page nine of this booklet. These successes include seven ITs which have been selected for Service, Agency, or limited Combatant Commander fielding (including fielding in support of Hurricane Katrina), two ITs which achieved milestones and continue spiral development as Programs of Record, one IT was selected for funding via a Congressional Plus-up for further research and development, and one IT that is being submitted as a Limited Acquisition Authority candidate.

OBJECTIVES 2005

- **MISSION ASSURANCE**
- **SITUATIONAL AWARENESS**
- **MULTI-LEVEL/MULTI-DOMAIN PROTECTION**
- **COLLABORATIVE INFORMATION ENVIRONMENT**
- **ISR DESSEMINATION**
- **WIRELESS SECURITY**
- **LANGUAGE TRANSLATION**
- **INTEGRATED LOGISTICS**

- CWID 2005, including setup and rehearsal, ran from 31 May until 24 June, 2005. Scenario execution started 13 June and continued until 24 June. Each "CWID Execution Day" totaled six hours from 1600 to 2200 Greenwich Mean Time (Zulu). Far more than a technology showcase, this year the demonstration proved again to be an effective venue for the U.S. to strengthen relationships with its day-to-day HLS/HLD partners and coalition nations. CWID continues to provide an opportunity to solve interoperability shortfalls and gaps on a wide array of systems.

UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS

RECOMMENDATIONS

Outstanding trials, CWID 2005

The trials listed below are top performing warfighter/operator technologies as recommended by the CWID Senior Management Group (SMG).

NOTE: Trials are listed in order of trial number.

TOP PERFORMERS

HISTORICAL EVOLUTION

From Concept to Frontline

CWID traces its history to the establishment of the U.S. Army's Secure Tactical Data Network in the early 1980s.

The early Secure Tactical Data Network (STDN) efforts concentrated on U.S. Army (USA) - only issues and incorporated multi-service command, control, communications and computer (C4) challenges beginning with STDN 3. The Joint Staff recognized that advances in C4 technologies in the public sector were outpacing DoD capabilities and decided to harness the STDN effort to enhance the military's transformation.

In 1993, the Joint Staff assumed sponsorship of the STDN series under the command, control, communication, computer and intelligence (C4I) for the Warrior concept. Using the Defense Information Systems Agency (DISA) as the Executive Agent, the Joint Staff directed DISA, in concert with a lead Service, to organize network experiments to bring emerging public sector, and other government agency technologies, into DoD projects and into the warfighters' sphere of recognition. DISA was concurrently directed to improve joint C4 interoperability.

In 1994, the annual STDN efforts evolved into the first JWID. The Air Force was the lead service and U.S. Atlantic Command was the host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality to joint and combined warriors. Key efforts in JWID '94 included the demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six weeks after the conclusion of JWID '94, GCCS was operationally deployed to U.S. Atlantic Command to support military operations in Haiti. Full operational deployment of GCCS to all combatant commanders occurred within twelve months after JWID '94.

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID assisted in this development through establishing itself as a coalition interoperability forum through invitations to the Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO beginning with JWID '94 and continuing to the present. While these invited participants use JWID to perform their own technology demonstrations and joint interoperability trials, their main intent is to promote and ensure C4 interoperability with the U.S.

EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to the warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year, with eventual fielding to combatant commands. JWID '98 fielded three Gold Nuggets to warfighters, selected from the results of JWID '97.

Due to U.S. year 2000 (Y2K) concerns, JWID '99-R was revised to focus upon coalition interoperability trials between the U.S. and CCEB/NATO nations. To more easily promote such trials and other C4I experiments, the Coalition Wide Area Network (CWAN) established annually for JWID evolved into the standing CFBLNet. This flexible network permits C4I experimentation among the U.S. and nations of CCEB/NATO, on a year-round basis, using systems jointly owned and managed by CFBL membership.

JWID '00-'01 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations at multiple, worldwide sites. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) was refined and subsequently selected for worldwide fielding to the Unified Commands. JWID '01 DCTS trial execution and assessment permitted DISA to field the capability, within seventy-two hours, in support of DoD requirements follow-

ing the terrorist attacks of September 11th, to multiple networks.

COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to a full focus on coalition interoperability, led by U.S. Pacific Command (USPACOM), the host combatant commander. The demonstration included Pacific Rim nations in a Pacific Theater Initiative, with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Multiple coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportunities. In addition, the JWID CWAN continued use of CFBLNet architecture and services established in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device following JWID 2002.

JWID 2003 took coalition interoperability to new heights. USPACOM guided the MTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 included management of information exchange to a larger, more robust network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. JWID 2003 addressed multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange requirements. Another milestone featured DISA assuming duties as the lead agency, providing broad-base management support to JWID activities. Four Coalition Interoperability Trials (CITs) with especially noteworthy performance were submitted to USJFCOM J861, for consideration for the new J861 Transformation Change Package (TCP) fielding process.

HOMELAND SECURITY

JWID 2004 featured USNORTHCOM as the Host Combatant Commander bringing a Homeland Security/Homeland Defense focus to the demonstration. This approach broke new ground beyond the traditional JWID coalition interoperability area, adding government interagency information sharing. USNORTHCOM, in a departure from previous JWIDs, invited agencies within the Department of Homeland Security (DHS), including first-time participation for FEMA, the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau. Limited coalition participation between these organizations occurred as Canada's Office of Critical Infrastructure Protection joined in the interoperability trials. This activity offers significant potential for more extensive cooperation between other coalition homeland security organizations and their U.S. counterparts. JWID 2004 involved 25 countries, military services, and government agencies participating in a scripted scenario over a global network.

USNORTHCOM was host Combatant Commander in 2005 as the demonstration moves forward with a name change. Now CWID, shift from "Joint" to "Coalition" describes the larger community of participants, including national and international government agencies. A new name was not the only change for CWID in 2005.

USJFCOM formally assumed oversight for planning and execution of CWID 2005 from the Joint Staff in July 2004. This involvement brings USJFCOM advocacy for U.S. combatant command interoperability shortfall resolution to the forefront. USJFCOM's objectives include (1) ensure CWID demonstrates relevant technologies that address combatant commander capability gaps, (2) investigate military, coalition and interoperability solutions, (3) identify technologies suitable for prototype initiatives, and (4) rapidly deliver relevant technologies to the warfighter and, where appropriate, transition these technologies to Programs of Record.

CWID 2005 features revitalization of the planning and collaboration web site, including readily accessible general information. Online trial submission was created to abbreviate the initial proposal process for interested technology representatives. Additionally, CWID established a Concept of Operations (CONOPs) for all recurring aspects of the planning and execution process.

U.S. European Command (USEUCOM) will be host Combatant Commander for 2006 and 2007.

ASSESSMENT

Providing Objective Trial Review

The Assessment Working Group (AWG) charter is to provide the Joint Staff, Command/Services/Agencies, and other interested parties with an objective assessment of qualifying interoperability trials with respect to warfighter/operator utility, interoperability and Information Assurance (IA).

The ultimate goal of the assessment effort is to identify those trials that are the best candidates to provide solutions or enhancements to C4 interoperability challenges facing Joint, Coalition, HLS and HLD operations in the near term while protecting the operational networks data and integrity.

The AWG organization is comprised of three analyst teams that provide three different categories of assessments: Warfighter/Operator Utility, Interoperability, and Security Capability. These analyst teams are comprised of representatives from the CWID Joint Management Office (JMO), Joint Interoperability Test Command (JITC), National Security Agency (NSA) and Coalition nations. Each analyst team scrutinizes the ITs based on predefined criteria to determine the level of assessment that can be performed. Each trial has the potential to receive any combination of the three assessment types or none at all.

For CWID 2005, the SMG was responsible for prioritizing participating ITs. To support each trial's assessment level, the AWG considered this prioritized list along with each trial's nature, maturity level, and assessment constraints. For trials that did not qualify for a formal assessment during CWID, the AWG coordinated with the Systems Engineering and Integration Working Group (SEIWG) to ensure that a summary report was provided (when applicable) to document the results of CWID execution.

During the two week CWID execution period, AWG representatives highlighted problems/issues and any corrective actions for each IT. This information, along with firsthand warfighter/operator input collected through the Joint Systems Integration Command (JSIC, formerly Joint Battle Center, or JBC) Data Collection and Analysis Tool (JDCAT) and the results of their advertised data exchanges captured within the WISE (Web Information Services Environment) Interoperability Collection and Assessment Tool (WICAT), were consolidated to complete the CWID assessment report for qualifying trials.

The final assessment report highlights the IT's performance with regard to meeting original stated goals as well as Warfighter/Operator Utility, Interoperability, and IA objectives.

The enhanced cooperation across U.S. and coalition assessment activities increases the validity of the assessment process and provides

the opportunity to apply CWID's promising technologies to the operational environment.

WARFIGHTER/OPERATOR UTILITY ASSESSMENT PROCESS

The warfighter/operator assessment focused on the trial's "value added" to the warfighter/operator, its technical performance and the ability to meet stated objectives and capabilities in support of the CWID objectives in an operational environment.

During CWID execution, warfighters/operators and staff personnel operated and interacted with the trials and evaluated the systems utility by completing CWID network-accessible questionnaires generated via JDCAT. The questionnaires were specifically developed for each trial based on:

- Objectives mapped back to the CWID objectives
- Predefined MSEL events and/or definitive test schedules
- Trial capabilities
- Applicable Measures of Performance tailored to each trial

INTEROPERABILITY ASSESSMENT PROCESS

The Interoperability/Technical assessment focused on the trial's ability to exchange usable data with CWID Network core/component services or other trials. Prior to execution, JITC worked with each trial's staff expert to define the system interfaces that would be exercised and how these interfaces and anticipated data exchanges mapped to CWID objectives. These definitions were developed into Information Exchange Requirements (IERs). IERs define: what information is exchanged, who exchanges the information, why the information is necessary, and how the exchanges take place.

During execution, the Interoperability Assessment team observed these predetermined exchanges, ensuring that the data transferred is received and processed correctly by the receiving system. Results were documented in the WICAT database developed by JITC. All information collected by JITC can be applied to the formal U.S. interoperability certification process, leading to faster fielding of products demonstrated during CWID.

SECURITY ASSESSMENT PROCESS

The security assessment focused on how the trial counters identified threats and enforces identified policies consistent with appropriate usage assumptions for the projected warfighting environment. The Security Environment Elements are threats, assumptions and policies which a system or product might affect within that environment. Each assessed trial was documented for how well it countered the environment threats and enforces the environment policies consistent with the assumptions for how the capability is intended for use

The security assessment process contained three major phases. The first phase was conducted throughout the planning process and resulted in the documentation of threats and mitigation activities for each trial receiving a security assessment. Phase two consisted of basic security tests performed during CWID execution. In the final phase, selected IA related trials received assistance developing documentation to facilitate a formal evaluation through a Common Criteria Testing Laboratory.

CWID NEXT STEPS

Forty-eight ITs participated in the CWID 2005 event, of which 44 received various levels of formal review involving warfighter, interoperability and security assessments. Thirty one ITs received a warfighter assessment, 29 a JITC interoperability assessment and 19 an NSA security assessment. The SEIWG conducted technical assessments on the remaining ITs to establish a performance baseline for future reference. Assessments generated during CWID 2005 are useful for industry marketing and research efforts while providing Combatant Commanders/Services/Agencies (C/S/A) an opportunity to evaluate the utility of cutting edge technologies. USJFCOM reviews and evaluates IT assessments to identify those promising solutions that may be considered for transition to the warfighter via selected DoD funding programs or as a Limited Acquisition Authority candidate.

INTRODUCTION
UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS

CWID 2005 Demonstration Successes

Trials listed below continue development actions as described in the subheadings. Trial assessment summaries start on page 11 of this booklet. Full assessment documentation is on the companion Compact Disk, located on the inside front cover.

LIMITED ACQUISITION AUTHORITY CANDIDATE

TRIAL NO.

03.70 Multi-level-secure Information Infrastructure (MI2):

- USNORTHCOM sponsored demonstration that addressed HLS/HLD information sharing and information assurance shortfalls; subject of a pending Limited Acquisition Authority request to USJFCOM.

FURTHER TESTING

05.44 Advanced Geospatial Imagery Library Enterprise (AGILE):

- Successfully demonstrated JPEG2000 technology to expedite the transfer of large image files; is undergoing JSIC assessment for continued development for military applications and assessment as part of the Joint Systems Baseline Assessment (JBSA).

05.74 Posted Applications over Return Channel Satellite:

- USAF sponsored, DISA technology, successfully evaluated for certification in JUICE '06.

CONGRESSIONAL PLUS-UP

01.75 Masking Shunt (MS100SC):

- Innovative technology jointly sponsored by DISA – New Zealand; provides second layer defense against internet intruders by masking the server or computer MAC address; Masking Shunt has undergone testing at DISA's Slidell site, Louisiana, and is funded through a Congressional Plus-up for further research and development by the Office of Naval Research at the Joint National Training Center.

PROGRAMS OF RECORD

02.09 Commercial Joint Mapping Tool Kit (CJMTK):

- NGA sponsored program of record that participated to accomplish selected milestones while validating web-services and implementations as the solution matures to support network-centric enterprise service security and discovery services.

02.47 Joint Warning and Reporting Network (JWARN):

- Part of the Joint Program Office for Chemical and Biological Defense; accomplished scheduled milestones and is undergoing further assessment as part of the Deployable Joint Command and Control (DJC2) initiative.

LIMITED COMBATANT COMMANDER FIELDING

03.91 One Way File Transfer (OWFit):

- USJFCOM sponsored technology proposed for use in USCENTCOM; projected delivery to JSIC Feb '06 for assessment prior to potential deployment.

04.88 Incident Commanders' Radio Interface (ICRI):

- USNORTHCOM-sponsored solution that successfully enabled disparate "legacy" radio signals to be transformed into single-site communication; successully deployed in support of hurricane Katrina relief efforts; DHS purchased the systems and made it available via the Commercial Equipment direct Assistance Program to local public safety agencies.

SERVICE FIELDING

01.61 Marine Air Ground Task Force Continuity of Operations (MAGTF COOP):

- Emerging USMC program of record currently supporting units in the field; the solution validated ongoing developmental attributes and showcased the solution for possible expanded DoD implementation.

02.55 Tactical Medical Coordinating System (TacMedCS):

- USMC developed and sponsored solution to enhance the management of battlefield casualties from injury to release; the solution combines a handheld device and SAT data modem and has undergone a limited fielding; was deployed on USS Comfort to support hurricane relief efforts.

03.93 Multi-Level Chat (MLC):

- USJFCOM sponsored solution approved by DSAWG for use in Trident Warrior '06 and retention by the Navy for operational use; MLC, as part of CDCIE.

AGENCY FIELDING

02.42 Pliable Display Technology (PDT):

- NGA sponsored solution that enables a Rapid Access Image Viewer and Mobile Access Image Viewer to support JPEG2000 wavelet compression in a constrained bandwidth environment; CWID participation contributed to NGA purchase decisions and continued development.

03.68 ARINC Wireless Interoperability Solutions (AWINS):

- NGB sponsored solution used to transform VHF, UHF and Cell Phone communications into single-source Voice over IP; the technology was successfully used by Louisiana government activities in support of hurricane Katrina relief efforts.

05.44 Advanced Geospatial Imagery Library Enterprise (AGILE):

- NGA prototype that is subject to an ongoing JSIC Joint Military Utility assessment and is being used in the field today.

04.88 Incident Commander's Radio Interface (ICRI) – see description above

INTRODUCTION
UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS

Perspectives

The U.S. Air Force and U.S. Atlantic Command undertook the first formal Joint Warrior Interoperability Demonstration (JWID) in 1994, followed by the U.S. Marine Corps and U.S. Pacific Command in 1995. Technologies and terminologies in common use now debuted then, including Common Operational Picture (COP), Asynchronous Transfer Mode (ATM), Global Broadcasting System (GBS) and Multi-Level Security (MLS).

U.S. ARMY LEADS

1996 *with U.S. Central Command*

- Joint Total Asset Visibility
- Common Operational Modeling, Planning and Simulation Strategy (COMPASS)
- Global Command and Control System (GCCS)
- Common Operational Picture (COP) validation

U.S. NAVY LEADS

1997-1998 *with U.S. Atlantic Command*

- Interoperability mandated in Joint Vision 2010
- Invited Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand, United Kingdom)
- Common Operational Modeling, Planning and Simulation Strategy (COMPASS)
- Increased Compression Engine (ICE)
- Radiant Mercury Imagery Guard

U.S. AIR FORCE LEADS

1999-Revised *with U.S. Joint Forces Command (formerly U.S. Atlantic Command)*

- U.S. Y2K concerns drove revision to exclusive CCEB nations and NATO network support
- Combined Wide Area Network (CWAN) transition to Combined Federated Battle Lab Network (CFBLNet)
- COP Interface exchange
- eXtensible Markup Language (XML) viewing of the Air Tasking Order (ATO)

2000-2001 *with U.S. Space Command*

- Silent Runner® and PATROL© Gold Nuggets fielded

1995, 2002

1996

1997, 1998

1999 to 2001

2003

2004, 2005

2006, 2007

- Emphasis on Coalition Interoperability Trials (CITs)
- Support from National Geospatial-Intelligence Agency (NGA)
- Defense Messaging System (DMS)
- GCCS first COP exchange with Allied networks

U.S. MARINE CORPS LEADS

2002 *with U.S. Pacific Command*

- Inclusion of Pacific Rim nations in Pacific Theater Initiative
- Comprehensive assessment methodology
- Language translation services in an instant messaging format

DEFENSE INFORMATION SYSTEMS AGENCY NAMED PERMANENT LEAD AGENCY

2003 *with U.S. Pacific Command; transition assistance, U.S. Marine Corps*

- Dual domain network to accommodate different security access groups
- Core services led/supported by coalition nations
- Four Coalition Interoperability Trials candidates advanced to U.S. Joint Forces Command for TCP development

2004 *with U.S. Northern Command; U.S. Joint Forces Command observes in preparation for assumption of oversight summer 2004*

- Homeland Security/Homeland Defense (HLS/HLD) focus
- Continued emphasis on coalition interoperability
- Expanded coalition definition includes interagency HLS partners and allied militaries
- Greater levels of demonstration complexity

2005 *with U.S. Northern Command; U.S. Joint Forces Command assumes oversight for planning and execution of CWID from the Joint Staff*

- Name change from "Joint" to "Coalition" to describe the larger community of participants, including national and international government agencies
- Revitalization of CWID planning and collaboration website
- Online trial submission to improve initial process
- Concepts of Operations (CONOPs) developed for the CWID planning and execution process

2006-2007 *with U.S. European Command*

INTRODUCTION
UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS

CONTENTS

Interoperability Trials

Trial assessment briefs appear on the following pages. For complete assessment documentation, go to the companion Compact Disk on the inside front cover of this booklet.

Trial numbering is based on objective numbers as follows:

OBJECTIVE 1: **MISSION ASSURANCE**

OBJECTIVE 2: **SITUATIONAL AWARENESS**

OBJECTIVE 3: **MULTI-LEVEL/MULTI-DOMAIN PROTECTION**

OBJECTIVE 4: **COLLABORATIVE INFORMATION ENVIRONMENT**

OBJECTIVE 5: **ISR DISSEMINATION**

OBJECTIVE 6: **WIRELESS SECURITY**

OBJECTIVE 7: **LANGUAGE TRANSLATION**

OBJECTIVE 8: **INTEGRATED LOGISTICS**

TRIALS
UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS

Interoperability Trials contents continued...

OBJECTIVE 7: LANGUAGE TRANSLATION (no trials)

OBJECTIVE 8: INTEGRATED LOGISTICS (no trials)

Trial assessment briefs appear on the following pages. For complete assessment documentation, go to the companion Compact Disk on the inside front cover of this booklet.

Trial numbering is based on objective numbers as follows:

OBJECTIVE 1: **MISSION ASSURANCE**

OBJECTIVE 2: **SITUATIONAL AWARENESS**

OBJECTIVE 3: **MULTI-LEVEL/MULTI-DOMAIN PROTECTION**

OBJECTIVE 4: **COLLABORATIVE INFORMATION ENVIRONMENT**

OBJECTIVE 5: **ISR DISSEMINATION**

OBJECTIVE 6: **WIRELESS SECURITY**

OBJECTIVE 7: **LANGUAGE TRANSLATION**

OBJECTIVE 8: **INTEGRATED LOGISTICS**

TRIALS

TRIAL CONTENTS

BOOKLET CONTENTS

IT01.01
Defense Message System

1. MISSION ASSURANCE ●

TRIAL OVERVIEW: The Defense Message System (DMS) is capable of providing coalition directory services supporting SMTP and military messaging. All national directory data is replicated and available to all coalition users, providing required information to support applications. Each nation uses a heterogeneous directory system to support internal messaging requirements. To support secure military messaging among allies using the ACP145 standard, nations synchronize data using LDAP Data Interchange Format (LDIF). This trial uses metatools to produce LDIF files from the U.S. Border Directory (BDSA) to send U.S. directory data to coalition partners, and to receive and upload coalition data. The trial also identifies directory schema compatibility issues between the U.S. X.500 and LDAP directories used to support the U.S. and its allies via the ACP145 gateway.

SPONSOR: DISA
TRIAL LOCATIONS:
NSWC Dahlgren
TRIAL PARTNERS:
N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Directory Services and Military Messaging Service Interoperability Trial received a SEIWG evaluation report.

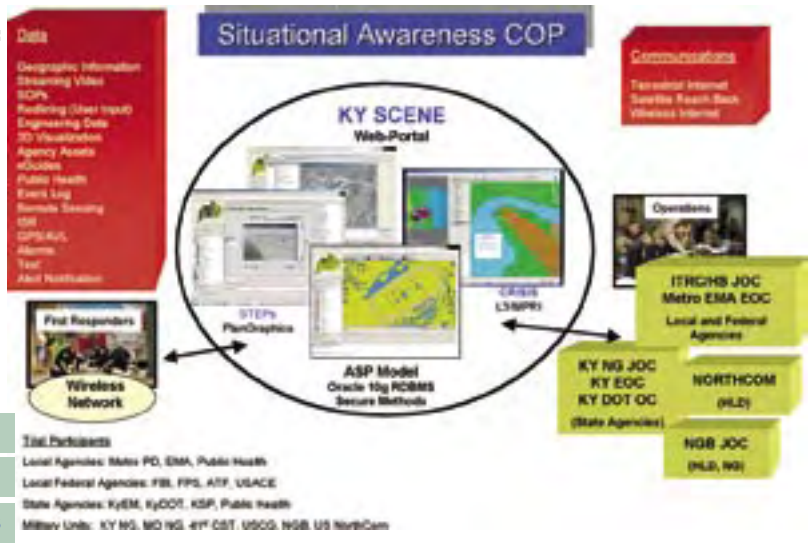
- DMS successfully demonstrated the viability of LDIF file transfers of directory data between the U.S. DMS directory system and allied partners' directory systems.
- DMS validated object classes and attributes necessary to support secure military messaging among allied partners.
- Identified directory schema compatibility issues between the US X.500 and coalition Military Messaging directory schemas.

IT01.20
Kentucky-Secure Collaborative Enterprise Network for Emergencies

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: Kentucky-Secure Collaborative Enterprise Network for Emergencies (KY-SCENE) is an interoperability solution developed by a team of organizations from the public, private and military sectors. It has the ability to provide users with a COP and real-time situational awareness information for use in response to an incident/event. Additionally, KY-SCENE can facilitate communication and information exchange between local first responders and support agencies, state agencies, federal agencies and military units. The trial demonstrates a replicable solution for local, regional or national response to a terrorist incident or natural disaster. The web-portal provides access to a variety of disparate information from multiple domains. Access to information is controlled by user authorization levels.

SPONSOR: NGB-CIO
TRIAL LOCATIONS:
USNORTHCOM
TRIAL PARTNERS:
N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Kentucky Secure Collaborative Enterprise Network for Emergencies Interoperability Trial received a Warfighter and Interoperability assessment.

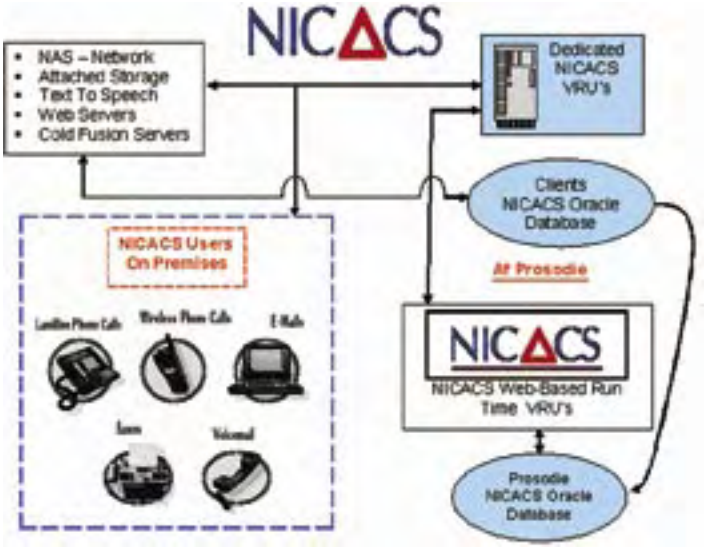
- KY-SCENE successfully demonstrated a unique single solution package of tools to enhance the first responder's situational awareness. Utilizing STEPS and the Watch Commander application, USNORTHCOM was able to participate and provide "real time" decision making support for events occurring over a thousand miles away in Kentucky.
- KY-SCENE demonstrated the ability to share locally gathered data between state level first responders and national level DoD warfighters requiring "Critical Incident Report" information.
- Utilizing web-portal technology, KY-SCENE provided live video, alerts, chat functionality, directories, mapping, photographic images, and process and procedures documents required by local first responders, state and federal agencies and military units.

IT01.40
National Incident Control & Action Communication System

1. MISSION ASSURANCE ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: National Incident Control and Action Communication System (NICACS) is designed to provide communication and alerting services between existing Public Switched Telephone Network (PSTN) phone, wireless, and Internet communication systems within and between diverse federal, state and local organizations of any size or composition. NICACS is unique because it combines cost-effective alerting/notification with a communications system to enhance effectiveness of internal personnel and enable collaboration between private or government agencies. NICACS has the ability to quickly disseminate information across multiple communication systems and multiple groups, agencies, or organizations without any added infrastructure.

SPONSOR: USCG
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT 04.15



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, National Incident Control and Action Communication System Interoperability Trial received a Warfighter assessment and a SEIWG evaluation report.

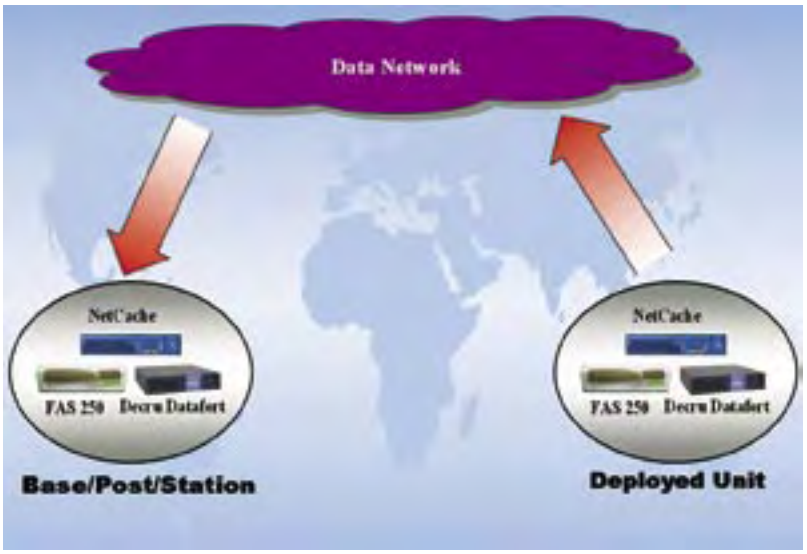
- NICACS successfully demonstrated increased HLS/HLD situational awareness between local, state, and federal agencies by broadcasting immediate emergency alert information via e-mail and plain old telephone service.
- While NICACS successfully demonstrated the ability to automatically recall personnel by sending cross-government alerts and correspondence and generating conference calls; it was unable to demonstrate the trials' planned Reverse-911 capabilities and collaborative planning across a bandwidth constrained operational environment.
- NICACS experienced server unavailability issues during the demonstration which made the system unreliable.

IT01.61
Marine Air Ground Task Force Continuity of Operations

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The Marine Air Ground Task Force Continuity of Operations (MAGTF COOP) is a suite of equipment designed to encrypt and replicate data while conserving bandwidth. This capability brings a common synchronized informational picture within the battle space. This suite includes the Network Appliance FAS250 which is a network storage device used to store local data and replicate data in real time to a remote site. Data is encrypted by the Decru DataFort using AES 256 encryption prior to the data being saved to the FAS250. The NetCache content delivery engine caches Internet web pages and streaming media; keeping the information closer to the user therefore saving valuable bandwidth.

SPONSOR: USMC
TRIAL LOCATIONS: NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Marine Air Ground Task Force Continuity of Operations Interoperability Trial received a Warfighter, Interoperability and Security assessment.

- MAGTF COOP system provided a successful solution to replicate large volumes of data from a Head Quarters to a Deployed unit in the field of operations by using encrypted keys with snap mirroring technology.
- MAGTF COOP successfully provided a means to synchronize data and provide backup redundancy, provide Mission Assurance capability by ensuring continuity of operations and improve overall warfighter situational awareness.
- MAGTF COOP's data encryption server added a level of security previously not seen.

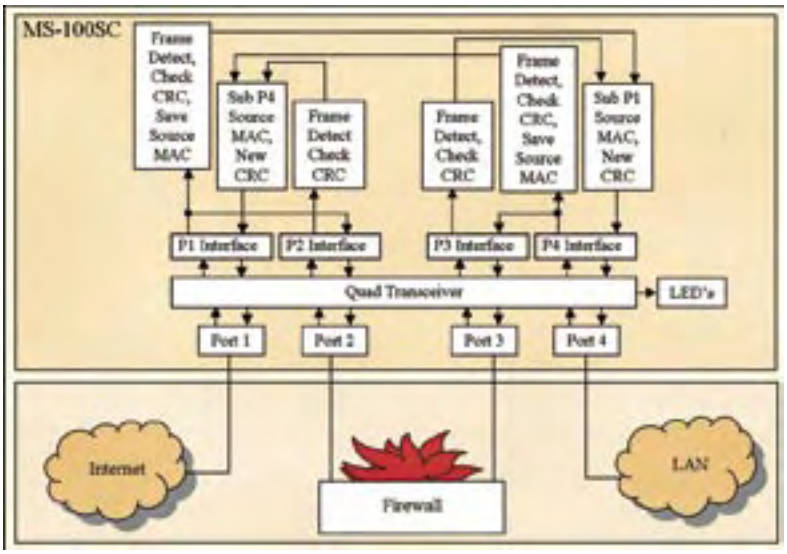
IT01.75
Masking Shunt

1. MISSION ASSURANCE ●

TRIAL OVERVIEW: Masking Shunt (MS100SC) is designed to finish the job that firewalls start. While any defensive structure, once detected, can eventually be defeated, those attempting to, can't target what they can't see. Firewalls and other defensive devices contain Media Access Control (MAC) addresses which can be and are being detected. These MAC addresses are statically assigned to each vendor and easily obtained via the internet. By "scrambling" the firewalls source MAC address and randomly replacing it with the MAC addresses of other devices, reliable detection of individual devices is no longer possible. Masking Shunt uses high speed FPGA technology to function without an operating system. This technology allows Masking Shunt to eliminate OS latency, vulnerabilities, OS bugs, and configuration problems while protecting firewall integrity.

SPONSOR: NZ
TRIAL LOCATIONS:
NSWC Dahlgren, SPAWAR, USEUCOM, AUS, NZ

TRIAL PARTNERS:
N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Masking Shunt Interoperability Trial received a Security assessment and a SEIWG evaluation report.

● Masking Shunt successfully demonstrated an extra level of security. When used in conjunction with other intrusion detection systems, Masking Shunt will help prevent unwanted discovery of local area networks for the purpose of spying or hacking.

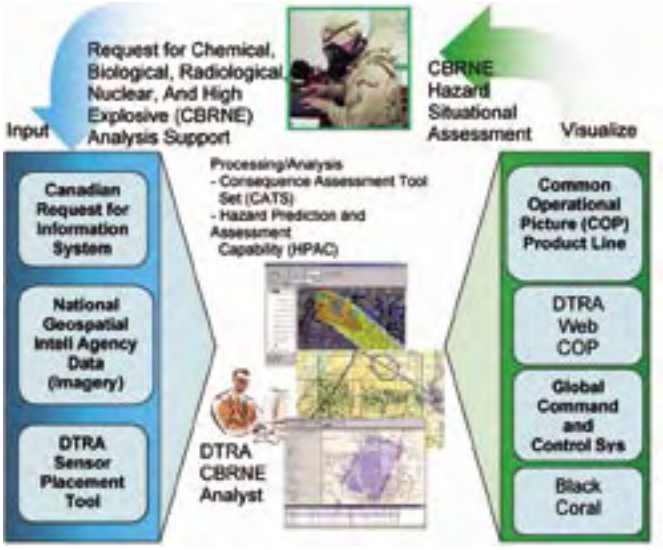
● Masking Shunt effectively hid the MAC addresses of network devices, making the MAC address appear to be another device by randomly replacing and changing the MAC addresses of the protected devices. This technique successfully prevented network and network device intrusion.

IT02.08
Weapons of Mass Destruction Common Operational Picture

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The Weapons of Mass Destruction COP (WMD COP) trial has the ability to integrate non-web and web enabled information sources and the capability to provide pre and post event WMD planning, assessment and visualization of WMD consequence management to military decision makers. The DTRA-developed sensor placement tool provides a plan for optimal placement of biological sensors. WMD COP demonstrates importing web based information (i.e. geospatial) from U.S. and allied/coalition organizations using DTRA's tools, titled Consequence Assessment Tool Set (CATS) and the Hazard Assessment and Prediction Capability (HPAC). WMD COP can facilitate an enhanced response to a WMD event and quicker analysis information dissemination within a coalition operating environment.

SPONSOR: DTRA
TRIAL LOCATIONS:
USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS:
IT02.30, 02.34, 02.65, 05.19, 05.24



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Weapons of Mass Destruction Common Operational Picture Interoperability Trial received a Warfighter and Interoperability assessment.

● Using DTRA modified ESRI software, WMD COP successfully demonstrated the ability to access and perform CBRNE analysis using geospatial data located on a Canadian ArcIMS server. This improved method permitted a more complete and faster analysis with a minimal amount of geospatial data actually being transmitted.

● WMD COP was able to provide plume data to several COP viewers including the DTRA WEB COP, IT 2.34 COP PL and IT 2.30 Black Coral. The level of information displayed in each of the three tools varied on the capability of the tool itself, but WMD COP was successful in providing each with a usable plume model.

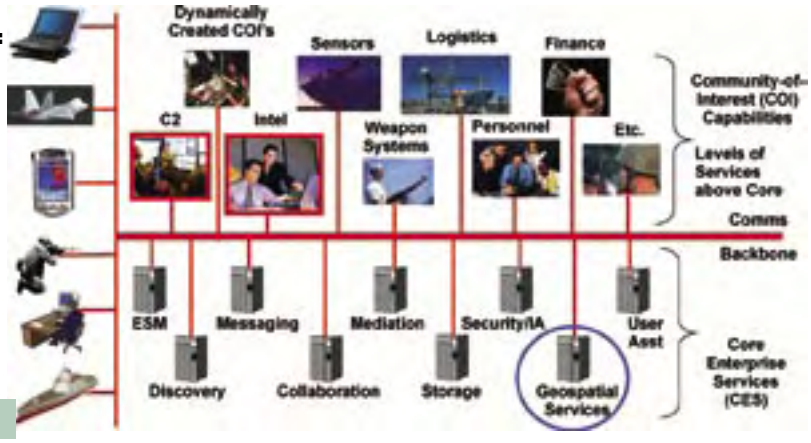
● Due to the absence of the CBRNE segment from the CWID GCCS build, WMD COP could not demonstrate electronically passing the plume model to GCCS. They were however, able to air-gap the Plume model to GCCS and display it in the COP.

IT02.09
Commercial Joint Mapping Tool Kit

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The NGA sponsored Commercial Joint Mapping Toolkit (C/JMTK) is market leading COTS software based on Environmental Systems Research Institute (ESRI) Arc Objects that has the ability to provide Mission Application Developers the building blocks to embed Command, Control and Intelligence capabilities in a stand-alone or integrated environment. These components offer sophisticated geospatial analytical tools that developers can use for desktop, web-based, or services based Mission Applications.

SPONSOR: NGA
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, NGA
TRIAL PARTNERS: IT05.19, 02.30, 05.24



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Commercial Joint Mapping Toolkit Interoperability Trial received an Interoperability assessment.

● C/JMTK successfully demonstrated the situational awareness objective by providing sophisticated geographic information systems (GIS) applications in a service-oriented architecture (SOA) accessible through the CWID network.

● C/JMTK successfully demonstrated three high-level GIS applications embedded within the toolkit.

1. Movement Projection (MP) application - provided vehicle routing selection based on given parameters.

2. Line of Sight (LOS) application - provided the capability to determine a number of different visibility products.

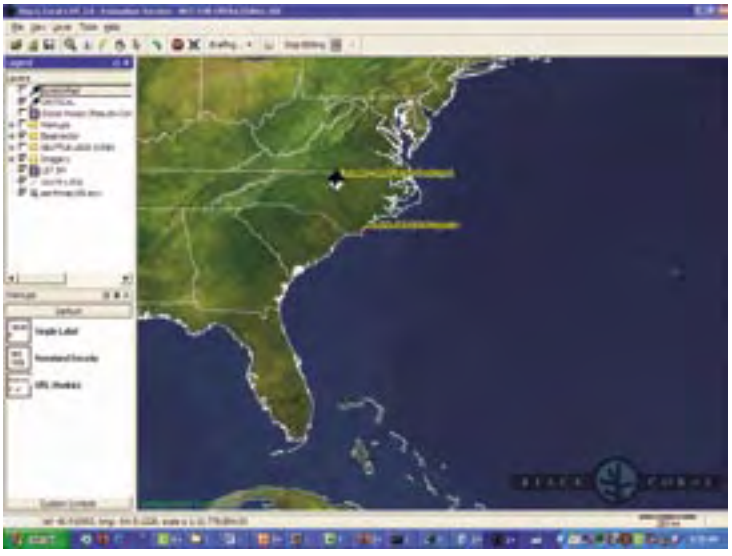
3. Positions of Advantage (POA) application - used to find geographic regions that met certain predefined criteria for landing zones and drop zones

IT02.30
Black Coral

2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: Black Coral LIVE addresses the difficulty that warfighters and first responders have using maps and imagery to increase their grasp of their situation. By collaborating with experts, they can now share a higher level of situational awareness in a collaborative environment.

SPONSOR: NGA
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, USEUCOM, NGA, CAN
TRIAL PARTNERS: IT02.30, 05.19



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Black Coral Interoperability Trial received a Warfighter and Interoperability assessment.

● Black Coral successfully received different types of geo-imagery files; Goegraphy Markup Language (GML), Raster Pattern Generator (RPG) raster and shapefiles to provide an enhanced collaborative mapping environment that promoted increased situation awareness.

● While Black Coral was successful, lack of support and training hampered its performance. Complexity, lack of training, and difficulties with initial setup discouraged role players from fully utilizing the tool.

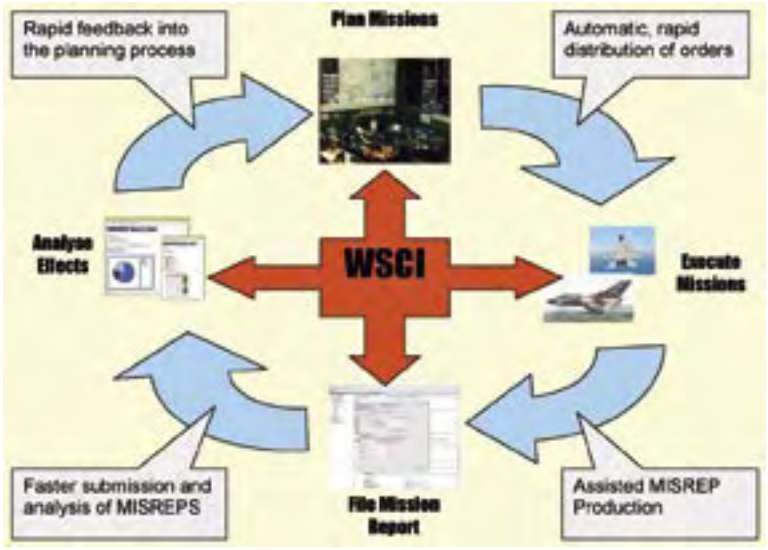
● Warfighters generally believed that Black Coral was a promising tool in combining collaborative planning and advance visualization capabilities, however, a more intuitive interface must be developed before it can be fielded.

IT02.33
Web Services for Coalition Interoperability

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Web Services for Coalition Interoperability (WSCI) is an information and security architecture that maximizes use of commercial web services technologies. It enhances availability and timeliness of information provided to air forces operating in a coalition environment. WSCI leverages fielded capabilities within the USAF and RAF, and the security design exploits the ability of the CWID network to provide assured separation of information. WSCI also incorporates a Mission Report (MISREP) management tool. Based on web services, it provides visualization capabilities to the commander and speeds up MISREP analysis, allowing more rapid evaluation of the effects achieved during an operation. WSCI facilitates the production and submission of MISREPs by coalition pilots, as well as making the final result available to all.

SPONSOR: UK
TRIAL LOCATIONS: Hanscom AFB, UK
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Web Services for Coalition Interoperability, Interoperability Trial received a Warfighter and Security assessment and a SEIWG evaluation report.

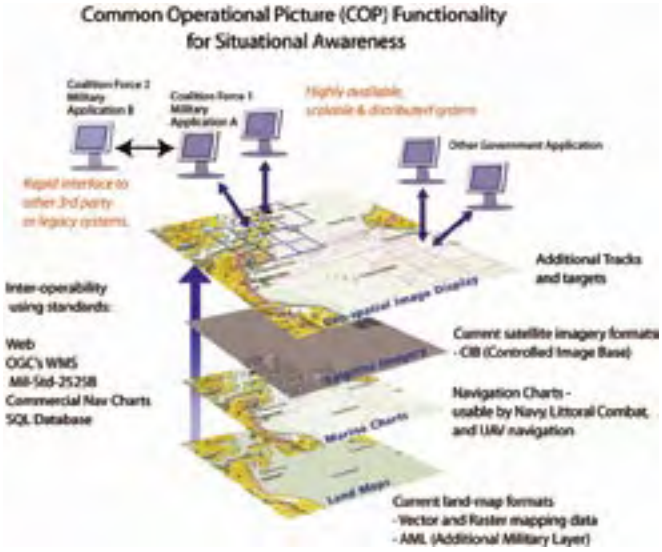
- WSCI exploited emerging Net-Centric Enterprise Services (NCES) technologies to enable rapid, on demand, and secure information exchanges by implementing XML Guards and firewalls as secure technology solutions for SOAP transactions and warfighter information access.
- Utilizing TBMCS 1.1.3 web service capabilities for coalition collaboration WSCI facilitated faster information transfers between coalition partners, and delivered the required situational awareness to the warfighter.
- WSCI demonstrated VPN technology with secure access controls to web services and security of information in transit between network nodes.
- WSCI provided an information and security architecture that enabled the automatic dissemination of the Air Tasking Order (ATO) to all coalition forces.

IT02.34
Common Operational Picture Product Line

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Common Operational Picture Product Line (COP PL) can provide an enhanced interoperable situational awareness capability. The system can be used to provide near real-time access to geo-spatial and tactical data for warfighters or intelligence operators in joint and coalition warfare environment to create and share a Common Operational Picture (COP). The image display (COPIDS) capability supports a broad range of military geospatial data products, rendering these products quickly and accurately in a composite image. The tactical display (COPTDS) is integrated with the image display and uses MIL STD 2525B symbology for near real-time track filtering and display. A web access layer (COPWDS) enables a browser based situational awareness capability and interoperability among joint and coalition forces.

SPONSOR: Canada
TRIAL LOCATIONS: NSWC Dahlgren, SPAWAR, Hanscom AFB, USEUCOM, CAN
TRIAL PARTNERS: IT02.30



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, COP PL Interoperability Trial received a Warfighter assessment and a SEIWG evaluation report.

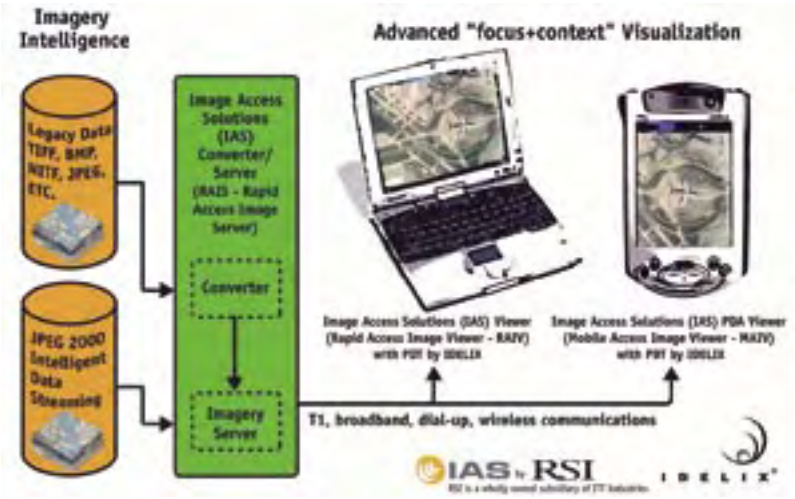
- COP PL successfully demonstrated enhanced situational awareness by providing near real time access to geospatial and tactical data for tactical, operational, and strategic warfighters or intelligence through a web-based COP.
- COP PL successfully demonstrated the toolsets' adaptability and flexibility by adding capabilities on the fly during CWID execution to meet operator requests for enhancements in functionality.
- Successfully Integrated MIL-STD-2525B symbology for near real-time track filtering and display.

IT02.42
Pliable Display Technology-enabled User Interfaces

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The Pliable Display Technology (PDT) enabled, Rapid Access Image Viewer (RAIV) and Mobile Access Image Viewer (MAIV) are a part of an image access solution (IAS) server-client architecture. With JPEG 2000 wavelet compression capabilities, this robust server-client architecture provides delivery, compression, storage and quick visualization of large geospatial images with limited bandwidth. The PDT lensing interface is incorporated into the IAS viewers to introduce advanced "focus+context" visualization and data streaming capabilities, enhancing situational awareness, and speeding exploitation and dissemination processes. Warfighters, intelligence analysts, and first responders have the ability to stream higher resolution imagery through the PDT lens for a selected region of interest, while maintaining visual connection to contextual surroundings.

SPONSOR: NGA
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, USEUCOM, AUS, CAN, NZ, UK, NGA
TRIAL PARTNERS: IT02.08, 02.09, 02.34, 03.70, 05.19, 05.44, 06.25



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Pliable Display Technology-enabled User Interfaces Interoperability Trial received a warfighter assessment and a SEIWG evaluation report.

- The RAIV and MAIV significantly reduced the time for tactical analysts, warfighters and first responders with limited bandwidth to retrieve large imagery and geospatial data on both PC and handheld devices. Using JPEG2000 wavelet compression technology to stream imagery information to the PDT lens it quickly disseminated large image files by selecting a region of interest with the PDT lens, for "detail on demand."

- Situational awareness was improved via the PDT enhanced user interface which enabled warfighters to efficiently exploit information by controlling the visualization tool while working directly with the data.

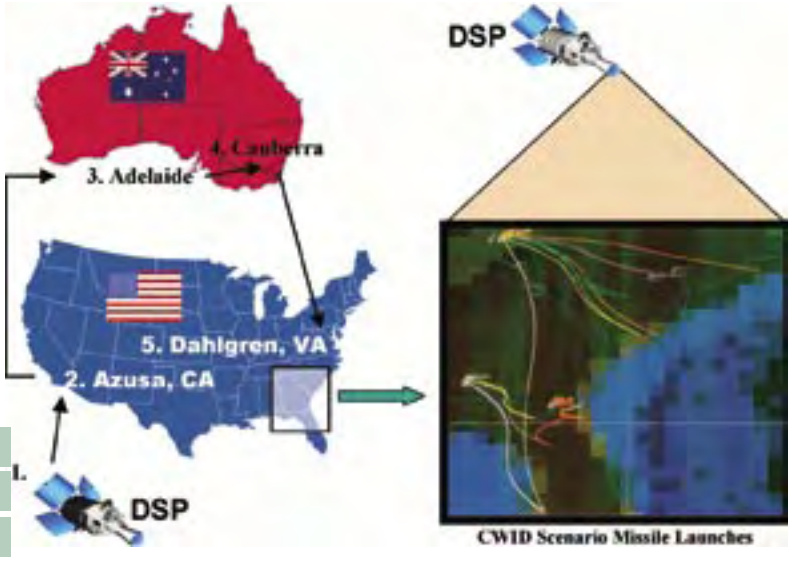
- PDT successfully supported the tactical warfighter requirement for examination of surveillance photos, mission planning, and battle damage assessment.

IT02.46
Coalition Infrared Sensor Ability

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The U.S. Defense Support Program (DSP) releases missile warning messages to provide warfighters with critical battlespace intelligence. The Coalition Infrared Sensor Ability (CISA) is designed to provide coalition nations the ability to pass key intelligence to U.S. and coalition warfighters by processing and releasing missile warning messages. Data from DSP satellites is sent from Azusa, Calif., to the Defence Systems Technology Office (DSTO), Adelaide, Australia. DSTO then uses the Australian Mission Processor (AMP) to process the data and release missile warning messages. Messages with critical Theatre Ballistic Missile (TBM) threat information is then forwarded to an Operations center for processing and further dissemination.

SPONSOR: USAF
TRIAL LOCATIONS: NSWC Dahlgren, SPAWAR, AUS
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Coalition Infrared Sensor Ability Interoperability Trial received an Interoperability assessment.

- CISA successfully provided real-time Space-Based Infrared Satellite (SBIRS) data from SPAWAR to Australia by sending, receiving and displaying TBM coordinates on the GCCS COP.

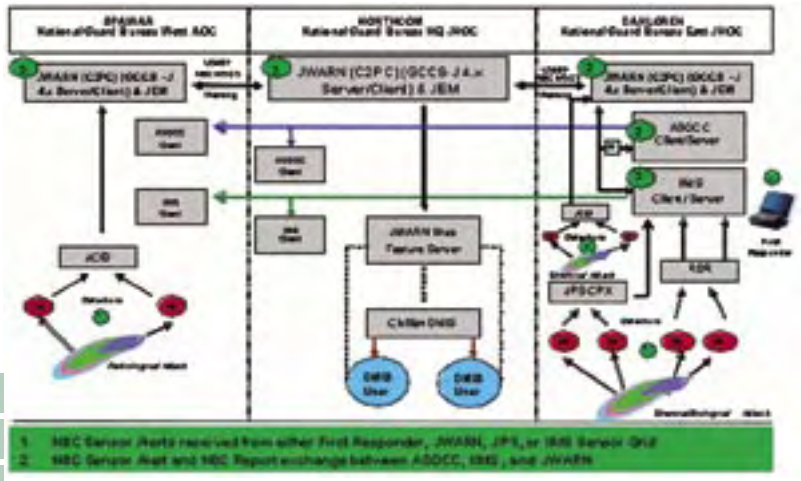
- CISA demonstrated the ability to detect and track missile launches and thus provided an enhanced interoperable situation awareness capability.

IT02.47
Joint Warning and Reporting Network

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Developed through the Joint Program Office for Chemical and Biological Defense (JPO/CBD), JWARN is designed to improve operations and survival in Nuclear, Biological and Chemical (NBC) environments. JWARN teams with two trials from JWID 2004: Area Security Operations Command Center (ASOCC) and Integrated Information Management System (IIMS) to demonstrate a standardized warning and reporting service that enables civilian and military CBRN information sharing. ASOCC provides real-time interoperable alerting, collaboration, and visualization capabilities for force protection and homeland defense, while IIMS helps fixed, expeditionary and incident response sites (air bases or ports) plan for, protect against, continue operations during, and recover from chemical, biological or conventional attacks.

SPONSOR: US Joint Staff
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT02.46



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Joint Warning and Reporting Network Interoperability Trial received a SEIWG evaluation report.

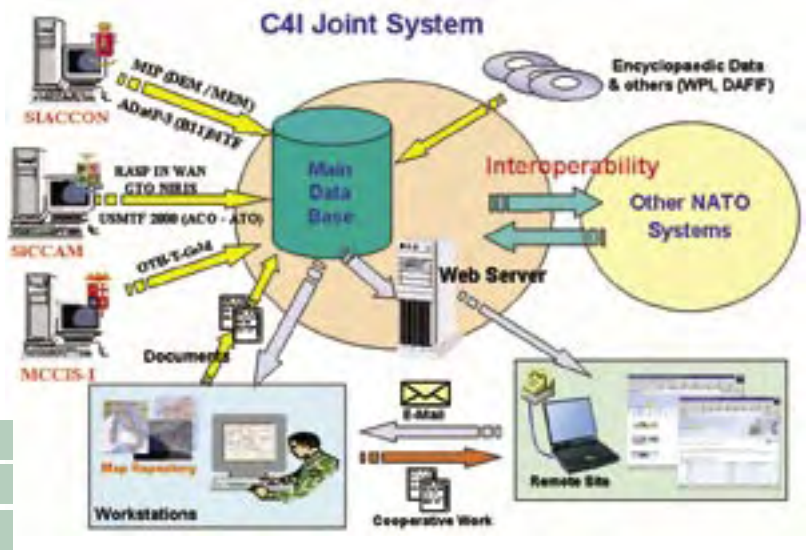
- During CWID 2005, Joint Warning and Reporting Network (JWARN) produced standardized warning and reporting services to enable civilian and military CBRN information sharing.
- Successfully integrated Command & Control and alerting systems including GCCS, C2PC, ASOCC, IIMS, and Web COP through the use of alert and NBC messaging capabilities. It provided a COP of CBRN events across disparate systems and organizations.
- JWARN successfully provided CBRN event planning capabilities including plume modeling and examination of emergency response infrastructure through the use of integrated military and civilian systems.

IT02.49
C4I Defence Joint System

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Italian C4I Defense Joint System is designed to provide top-level strategic capabilities, lying above the tactical functionalities offered by the command and control (C2) systems of each Armed Force. The trials objective is to test data and information exchange capabilities with other NATO, Partnership for Peace (pfp), U.S., Joint and single service C2 systems, by supporting high level C2 capability and COP exchange. C4I Defense joint system can test its capability to share COP in a multinational environment as GTF, OTH-G, and ADatP-3 messages. Italian Joint HQ and its Staffs can share COP and improve their situational awareness in a multinational environment.

SPONSOR: Gr.A.S.C.C/C2 Automation Group
TRIAL LOCATIONS: NSWC Dahlgren, NATO
TRIAL PARTNERS: IT02.50, 02.51, 02.52



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, C4I Defence Interoperability Trial received a Interoperability assessment.

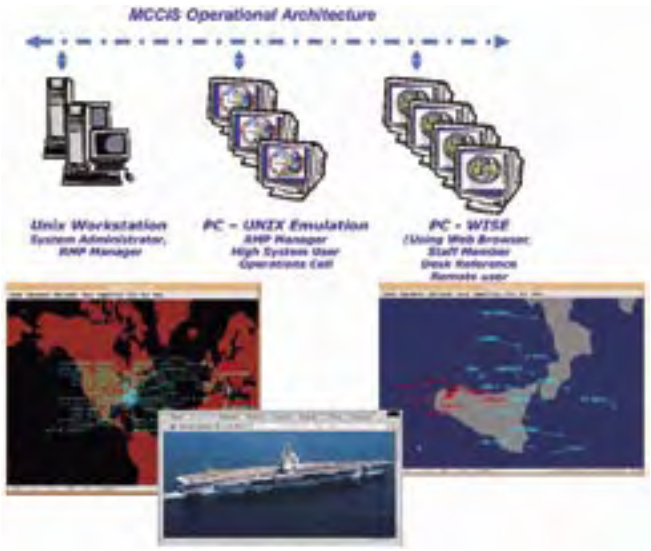
- C4I Defense provided OTH-Gold formatted JUNIT land and CTC/POS maritime track data that were successfully parsed and inserted into the GCCS-J and GCCS-A systems through the e-mail interface.
- C4I Defence received land, maritime and air track data from GCCS-J. JUNIT land tracks and CTC/POS Maritime tracks data were received in OTH-Gold format and sent directly to the Italian C4I system from GCCS via TCP/IP Socket 2020. The ATO and ACO was provided to the C4I systems in a USMTF format via email and manually inserted.
- There was a problem with ADatP-3 messages created using the GCCS BroadCast Enhancements (BCSTEN) Segment. The messages were created without following the standard context and therefore could not be received, parsed and inserted into C4I Defense without human intervention.

IT02.50
MCCIS-I

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The Italian Navy C2 System is designed to provide military users with reception of naval operational data in a multinational environment through OTH-Gold messages. The MCCIS-I System provides capabilities to acquire and manage data for scenario and situation evaluation. MCCIS-I system provides network services (email, chat, net meeting), Web browsing (access to databases, use of operational applications, easy Web page development), and Office Automation (document management, event management, news).

SPONSOR: Maritel
TRIAL LOCATIONS:
NSWC Dahlgren,
NATO
TRIAL PARTNERS:
IT02.49, 02.51, 02.52



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, MCCIS-I Interoperability Trial received a SEIWG evaluation report.

- Successfully demonstrated the capability to share the Recognized Maritime Picture (RMP) in a multi-national environment with other C2 systems through OTH-Gold messages.
- Successfully received and forwarded Naval information to the Italian C4I Joint System.
- MCCIS-I successfully exchanged maritime situational awareness information supporting CTC, PIMTRACK, JUNIT, and OVLY-2 Report formats. The MCCIS-I exchange of the XCTC Report format could not be achieved based on the inability of the GCCS-J system to process the XCTC Report Format.

IT02.51
SIACCON

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The SIACCON Command and Control System provides land operations planning and tasking, RLP reception and diffusion, message handling (ADatP-3 b11), and DB to DB replication mechanism (MIP solution). SIACCON automatically generates AdatP3 messages using data stored in GH4 Db as well as updating GH4 contents using those formatted messages. Graphically SIACCON has the ability to produce RLP in a VRML format in order to be suitable for systems not providing any specialized interoperability mechanism.

SPONSOR: Co.T.I.E
TRIAL LOCATIONS:
NSWC Dahlgren,
NATO
TRIAL PARTNERS:
IT02.49, 02.50, 02.52

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, SIACCON Interoperability Trial received an Interoperability assessment.

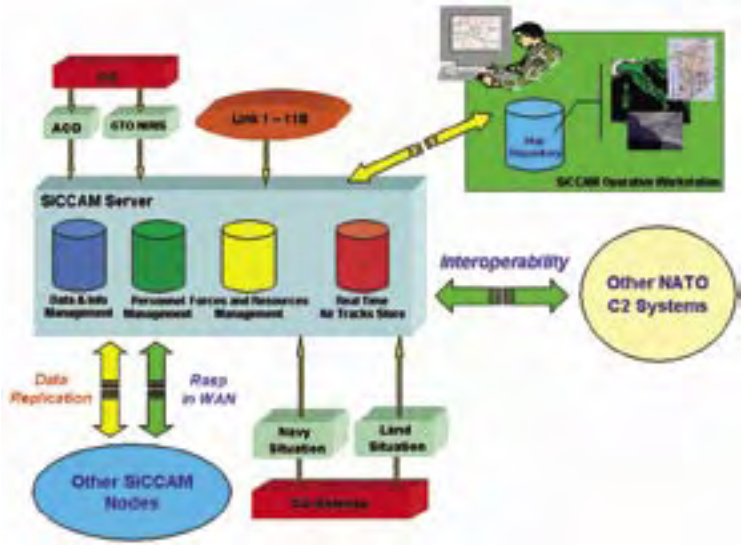
- SIACCON successfully sent three levels of land tracks to GCCS-A. ADatP-3 B11 formatted message containing Division, Brigade and Battalion track data were sent to GCCS-A via the e-mail interface.
- While a viewable SIACCON terminal at a U.S. site was not available to witness track data sent from GCCS-A to SIACCON, at NATO CWID the same test cases were performed with limited results. ADatP-3 messages generated by GCCS-A using the BroadCast Enhancements (BCSTEN) Segment do not follow the standard ADatP-3 format and could not be validated upon receipt by SIACCON. It took some modification by the SIACCON operator before the messages could be processed.

IT02.52
SiCCAM

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: SiCCAM is the Italian CCIS air system supporting the Italian JFACC (COFA) with the ability to plan and control air operations, and provide the Recognized Air Surface Picture (RASP). SiCCAM interfaces with other systems as subsystems, in order to build-up and present a near real time RASP for air planning and tasking through Airspace Control Orders (ACO) and Air Tasking Orders (ATO). SiCCAM monitors air missions and sensor data integration as well as providing air operations support functions to include: message handling, air mission planning, air mission reporting, situational awareness, airbase management, pilot readiness, resource management, metrology, logistics, and intelligence. Additionally, SiCCAM provides air track input to the COP while supporting the Joint and Unit level Commander.

SPONSOR: Co.T.I.E.
TRIAL LOCATIONS: NSWC Dahlgren, NATO
TRIAL PARTNERS: IT02.49, 02.50, 02.51



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, SiCCAM Interoperability Trial received a SEIWG evaluation report.

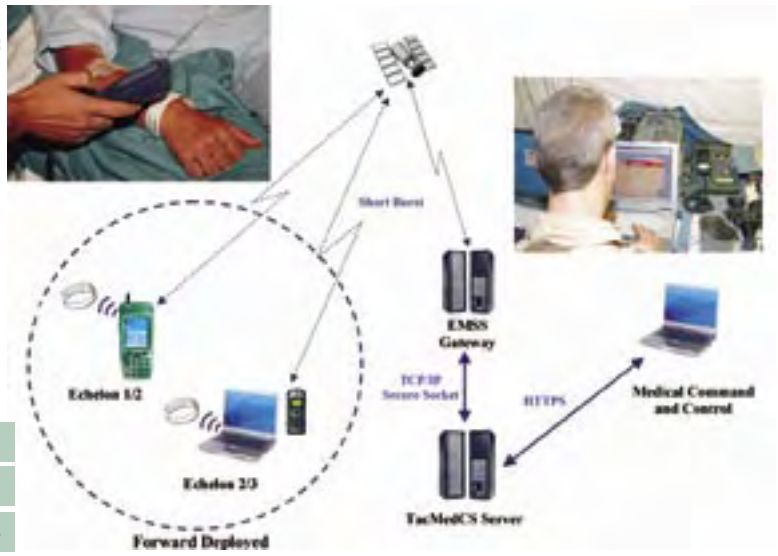
- SiCCAM successfully tested the tactical-level Command and Control (C2) systems data interchange between NATO, Partnership for Peace nations, and the US Theater Battle Management System (TBMCS).
- SiCCAM successfully received ACO and ATO global airspace management information messages as e-mail attachments utilizing the US Message Text Format (USMTF 2000).

IT02.55
Tactical Medical Coordinating System

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: TacMedCS captures and displays near real-time casualty data transmitted from the field. Information is displayed within a medical common operational picture (MedCOP) allowing both commanders and medical planners timely access to the information for enhanced medical situational awareness. The system uses Radio Frequency ID (RFID) technology and a satellite communications system to capture and transmit the data to a centralized database. TacMedCS is a web-based command and control application that reads and displays casualty information and generates statistical reports.

SPONSOR: USMC
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, NZ
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Tactical Medical Coordinating System Interoperability Trial received a Warfighter, Interoperability and Security assessment.

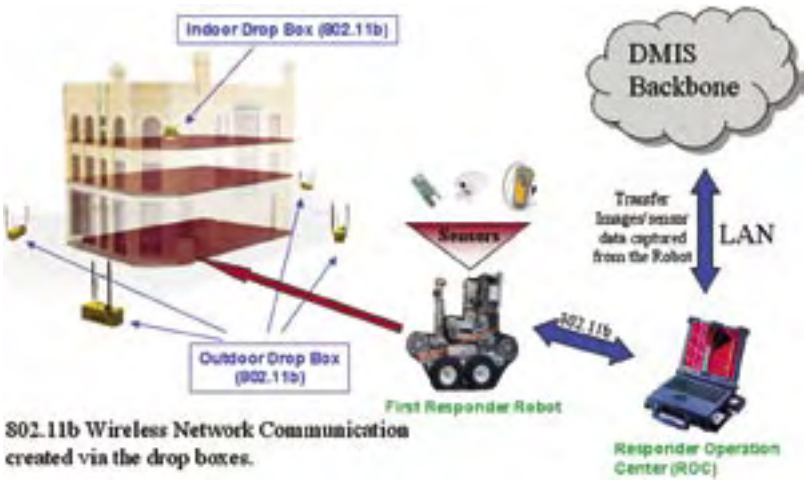
- TacMedCS successfully demonstrated the ability to provide commanders with increased medical casualty situational awareness by using Radio Frequency Identification (RFID) patient tags and scanners to input data. Data was transmitted (patient identification, location and casualty evacuation priority information) via satellite and populated the MedCOP database.
- Authorized users were able to access the TacMedCS database in the MedCOP, and view patient information and generate statistical reports. The web-based reports were easy to access and the ability to pull data into an Excel spreadsheet was extremely helpful.
- Warfighters unanimously said that this system would be helpful in medical resource planning.

IT02.58
First Responder Communication and Tracking System

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The First Responder Communication and Tracking System (FRCTS) is a modular, integrated, computer based system with advanced forward looking technology for wireless communications, position/navigation, information interchange, and power technologies. The system consists of wearable "First Responder Communicators" capable of delivering situational awareness information and intra-unit communication and collaboration; assisted GPS reference location nodes; a wireless 802.11b ad-hoc mesh network; and a mobile Responder Operations Center (ROC). FRCTS employs a First Responder Robot for entrance into an emergency environment which is capable of chemical gas and biological agents as well as performing various mechanical tasks as well as climb stairs at a 30 degree angle.

SPONSOR: US Army
TRIAL LOCATIONS: NSWC Dahlgren
TRIAL PARTNERS: IT02.77, 03.70, 04.26



802.11b Wireless Network Communication created via the drop boxes.

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, First Responder Communication and Tracking System Interoperability Trial received a Warfighter and Interoperability assessment.

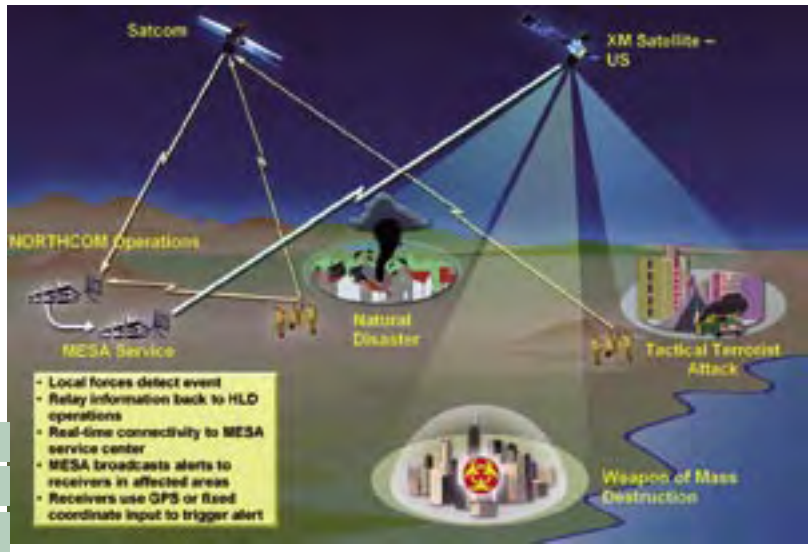
- Utilizing a robot and 802.11b wireless technology, FRCTS sent audio, sensor data, GPS location, and still video images to the robot operator who in turn forwarded the information through alert messages to other systems connected to DMIS backbone.
- The operator maintained excellent robot situational awareness via a four display screen.
- The robot has the capability to show first responders' positions inside a building but that capability was not demonstrated. Only robot position outside using GPS was monitored.

IT02.62
Mobile Enhanced Situational Awareness Network

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: MESA is an inexpensive data-casting suite that is designed to pass situational awareness information such as map and entity data, globally/or electively to any addressable warfighter echelon using commercial narrowband satellites (XM). The MESA network interfaces to existing unclassified networks for the purpose of global broadcasts of situation awareness information, alerts and warnings to addressable, low cost receivers for disadvantaged users, coalition forces, and 1st responders. The MESA architecture leverages readily available commercial satellite resources.

SPONSOR: USNORTHCOM
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Mobile Enhanced Situational Awareness Network Interoperability Trial received a Warfighter and Interoperability assessment.

- The MESA server operator successfully passed situational awareness data to the operators in the field units using COTS XM satellite receivers.
- The user-friendly display for alert messages and maps worked well. Warfighters were able to receive audio as well as text message alerts.
- The MESA Network was not considered a reliable source of situational awareness data. No uplink capability existed and therefore no means of acknowledging receipt of data was possible. In the event of a delivery failure, there was no means of easily determining what, if any, data was lost.

IT02.65
Regional Information Joint Awareness Network

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: The Regional Information Joint Awareness Network (RIJAN) is a communications network and visualization tool, based on open standards, that allows for sharing of information. RIJAN's primary goal is to support inter-agency communications, collaboration and internal networking and provide improved situational awareness and coordinated multi-agency response to a large-scale crisis. It is comprised of fixed and mobile sensors, nodes/gateways, critical incident management systems, common communication links, and operation centers all networked for enhanced vertical and horizontal inter-agency collaboration across local, state, and federal levels. The network allows for the use of diverse command and control applications, collaboration and decision-making tools.

SPONSOR: US Army
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: IT02.08

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Regional Information Joint Awareness Network Interoperability Trial received a Warfighter and Interoperability assessment.

- Successfully demonstrated a communications network allowing users from diverse agencies to communicate and share information easily, providing a common operational picture and collaboration capabilities for all users on that network. Collaborative sessions demonstrated the exchange of video, whiteboard and chat data.
- RIJAN did not demonstrate the ability to bring in new members or communicate with systems outside their network.
- RIJAN demonstrated the ability to hold collaborative sessions, using video, whiteboard and chat, but did not demonstrate the ability to bring in new members or communicate with systems outside their network.

IT02.77
Homeland Security Information Bridge

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Homeland Security Information Bridge (HSIB) is a web-based application that provides situational awareness by integrating the data from diverse sources and formats into a Situational Awareness (SA) map display. HSIB, as the host server, aggregates and fuses situational awareness data to create an integrated "common operational picture" display, posted to a designated website. Using HSIB's Dragonfly viewer, users with proper permissions can view the map display. However, an important feature available but not demonstrated during CWID 2005 is HSIB's open specification data format standards. This open specification standard allows other applications to retrieve HSIB data but use their own viewer for data display.

SPONSOR: US Army
TRIAL LOCATIONS: NSWC Dahlgren
TRIAL PARTNERS: IT02.07, 02.58, 03.70, 04.26

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Homeland Security Information Bridge Interoperability Trial received an Interoperability assessment.

- Successfully integrated data from diverse sources and formats into an Situational Awareness (SA) map display viewed via HSIB's Dragonfly viewer.
- HSIB successfully fused incident data from alerting systems, incident-reporting applications, and published DMIS CAP alerts to create a common operational picture for participants at all need to know levels within a single unclassified network.
- HSIB received air and maritime track data for situational awareness directly from IT 3.70 MI2 (Multi-level-secure Information Infrastructure trial) and integrated that track data as part of its common operational picture.

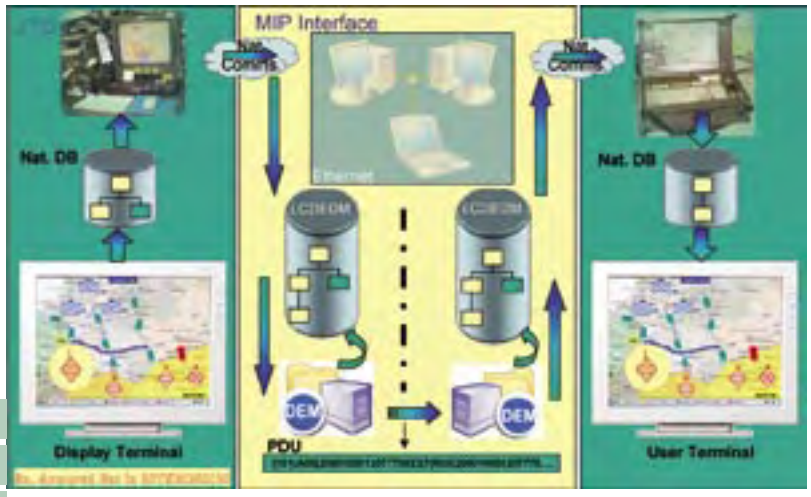
BOOKLET CONTENTS

IT02.83
Joint Tactical COP Workstation-USMC

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Joint Tactical COP Workstation (JTCW) represents an evolutionary migration of the Army Maneuver Control System (MCS) and the Marine Corps Command & Control Personal Computer (C2PC). JTCW resolves Blue Force Situational Awareness (BFSA) interoperability and capability gaps between the MCS and C2PC. Exchanging Blue Force Tracking data with coalition partners provides an improved BFSA and provides better identification of civilian concentrations and locations of US and coalition forces for operational planners. JTCW addresses the ability of the C2PC to seamlessly exchange information with Coalition Command and Control Information Systems (C2IS), enhance situational awareness visibility, improve doctrine, and facilitate decision-making and leadership options during an operation.

SPONSOR: PEO C3T/PM G CC2/Pdm MCS
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, NATO
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Joint Tactical COP Workstation - USMC Interoperability Trial received a SEIWG evaluation report.

- JTCW successfully demonstrated the integrated capability of the Command and Control Information Exchange Data Model (C2IEDM) to seamlessly exchange information with C2IS.

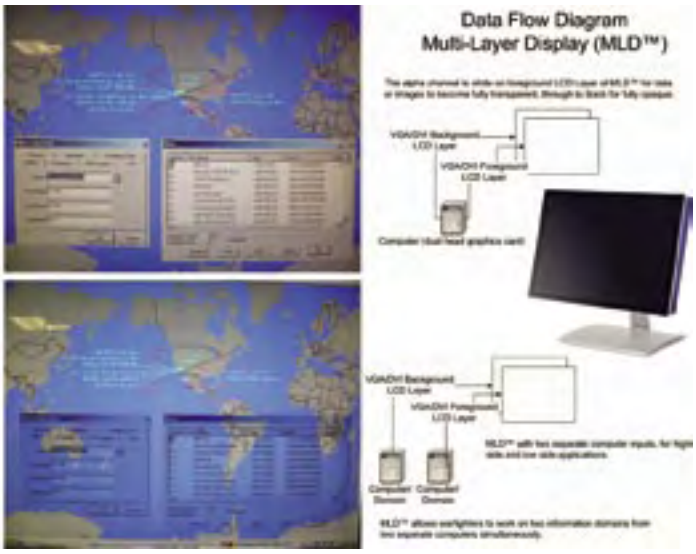
- JTCW successfully exchanged Land/Ground COP track data supporting Situation Awareness data with Coalition partners, in accordance with NATO specifications and demonstrated the feasibility of integrating the C2IEDM and Multi-lateral Interoperability Program (MIP) capabilities into the C2PC platform.

IT02.84
Multi-Layer Display

2. SITUATIONAL AWARENESS ●

TRIAL OVERVIEW: Multi-Layer Display provides a capability for viewing two computer screens at once on a single monitor, enhancing situation awareness by processing real-time operational information at a single desk position. The display provides a unique transparent 3-D depth display that overcomes the limitations of current 2D and 3D volumetric displays. Users simultaneously view screens with diverse applications and/or combinations of applications such as Geospatial Image displays, Collaboration tools, and Microsoft Document files.

SPONSOR: NZJF
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, AUS, CAN, NZ, UK, NATO
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Multi-Layer Display Interoperability Trial received a Warfighter and Interoperability assessment.

- Successfully demonstrated the ability to display two differing computer applications at the same time on a single monitor.

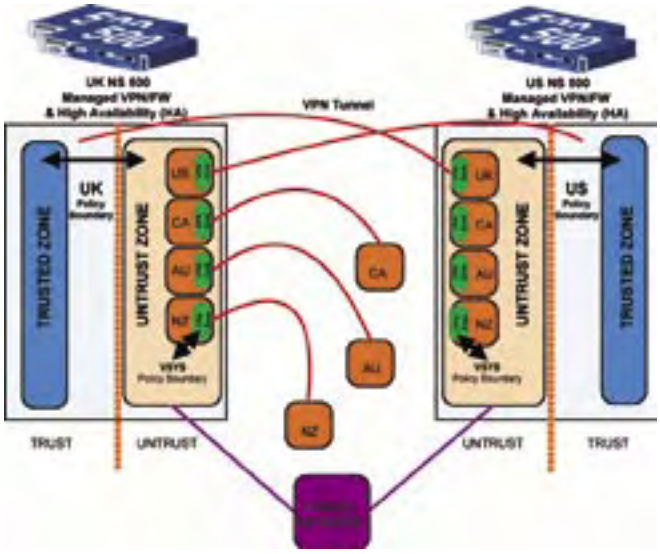
- Some combinations of file types did not display well and users found them hard to read and somewhat confusing.

IT03.13
Netscreen Security Products

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: Juniper Networks (NS-500) provides an integrated security system with a flexible, high-performance solution for large enterprise central sites and service providers. Its network security system integrates firewall, Denial of Service (DoS), virtual private network (VPN), and traffic-management functionality in a low profile, modular chassis. The flexible and resilient hardware architecture incorporates modular physical interfaces, redundant power supplies, fans, and high-availability interfaces. NS-500 provides high levels of total throughput for firewall and VPN, plus support for virtual systems and security zones. It supports defining and enforcing information flow policies among network nodes, ensures auditing of security relevant activities, offers protection from potential attacks, and provides the security tools to manage all of the security functions.

SPONSOR: DISA
TRIAL LOCATIONS: NSWC Dahlgren, SPAWAR, Hanscom AFB, USFK, AITS-JPO, AUS, CAN, NZ, UK
TRIAL PARTNERS: IT01.01, 02.33



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Juniper's Netscreen Security Products Interoperability Trial received a Security assessment and a SEIWG evaluation report

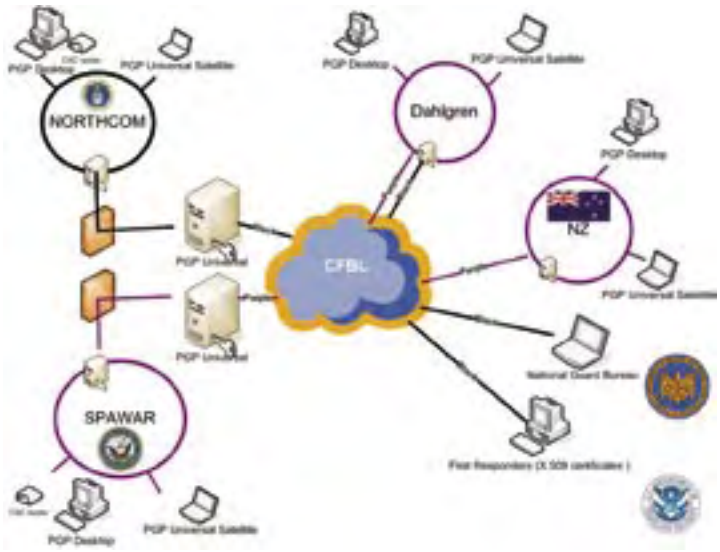
- Netscreen successfully demonstrated secure information exchanges across multiple security domains and communities of interest (COI) with AES 256-bit encryption.
- Using IPSec, Netscreen successfully passed data traffic through VPN tunnels and provided a VPN architecture to allow for multiple levels of security dictated by coalition relationships enhancing situational awareness, mission assurance and multi-level/multi-domain protection.
- Netscreen is Evaluation Assurance Level (EAL4+) certified for the firewall component. The VPN portion of the devices is under evaluation for EAL4+ certification.

IT03.29
PGP Universal

1. MISSION ASSURANCE ● 3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: PGP Universal represents a security architecture that transparently shifts the burden of securing e-mail messages and attachments from the desktop to the network transport protocol. PGP Universal, a drop-in, server-based, security solution that works with existing e-mail infrastructures, provides end-to-end or gateway-to-gateway message security. PGP Universal acts as an e-mail proxy or relay and either relays or delivers outbound e-mail. The system institutes security policies and makes decisions whether to encrypt or not to encrypt e-mail and enables secure communications across organizational boundaries without compromising privacy, security, or confidence. PGP Universal uses digital signatures to ensure transferred data originates from authenticated senders, while protecting against tampering, spoofing, and unauthorized interception.

SPONSOR: SPAWAR
TRIAL LOCATIONS: SPAWAR
TRIAL PARTNERS: IT01.20



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, PGP Universal Interoperability Trial received a Security assessment and a SEIWG evaluation report.

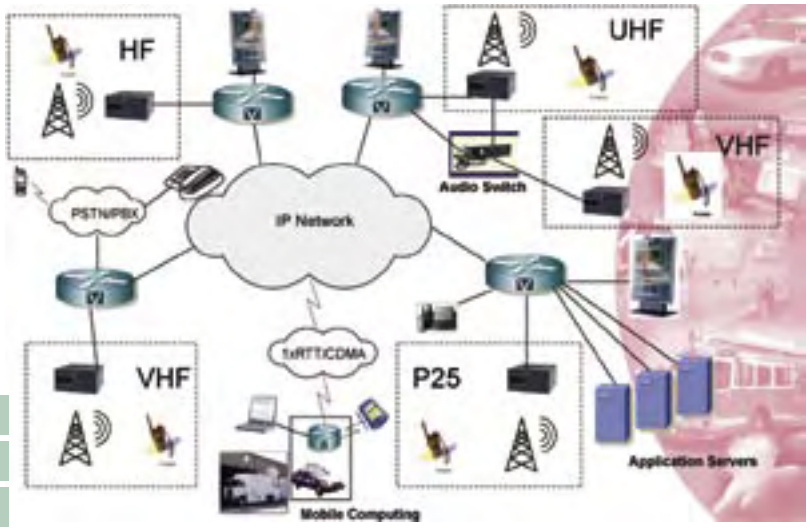
- The trial provided a comprehensive and self-managing security architecture entirely automatic and policy-managed, operating without the need for warfighter or system administration intervention. PGP Universal provided automatic key generation and life cycle management making wide-scale deployment practical and satisfying mission assurance objectives.
- PGP did not demonstrate activity with mobile CAC users and therefore, was not successful in meeting the CWID Wireless Security objectives.

IT03.68
ARINC Wireless Interoperability Solution

3. MULTI LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: ARINC Wireless Interoperability Network Solution (AWINS) is an integrated design of COTS products to resolve interoperability among disparate radio, telephony, and digital technologies within a single network domain. The architecture uses IP standards and VoIP as a common platform to provide interoperability across disparate radios, bands, frequencies, and telephone technologies.

SPONSOR: NGB
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, ARINC Wireless Interoperability Network Solution Interoperability trial received an Interoperability assessment.

- AWINS successfully demonstrated the ability to integrate dissimilar radio, voice, and communication systems on one data infrastructure by using IP standards and VoIP as a common platform, satisfying the ability to facilitate information sharing.
- AWINS successfully connected disparate radios and voice communications devices into a single conference call allowing users to communicate directly one- on-one or linking specific groups together.

IT03.70
Multi-level-secure Information Infrastructure

2. SITUATIONAL AWARENESS ● 3. MULTI LEVEL/MULTI-DOMAIN PROTECTION ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ● 5. ISR DISSEMINATION ●

TRIAL OVERVIEW: Multi-level-secure Information Infrastructure (MI2) provides information sharing within and across multi-level security information domains, enhanced situational awareness, and ISR dissemination. The MI2 infrastructure technology provides interoperability between disparate organizations operating at different security levels. MI2 combines three technologies, a middleware information management technology (Total Domain (TD)), a single direction guard solution (Tenix Interactive Data Diode (IDD)), and a multi-directional route guard (Boeing Secure Network Server (SNS)). The combination of these technologies facilitates retrieval, updating, data filtering, and information sharing simultaneously across multiple security domains. MI2 provides capabilities enabling efficient Information Management (IM) and Information Assurance solutions for data sharing.

SPONSOR: USNORTHCOM
TRIAL LOCATIONS: USNORTHCOM, SPAWAR
TRIAL PARTNERS: IT02.58, 02.77

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Multi-level-secure Information Infrastructure Interoperability Trial received a Warfighter, Interoperability, and Security assessment.

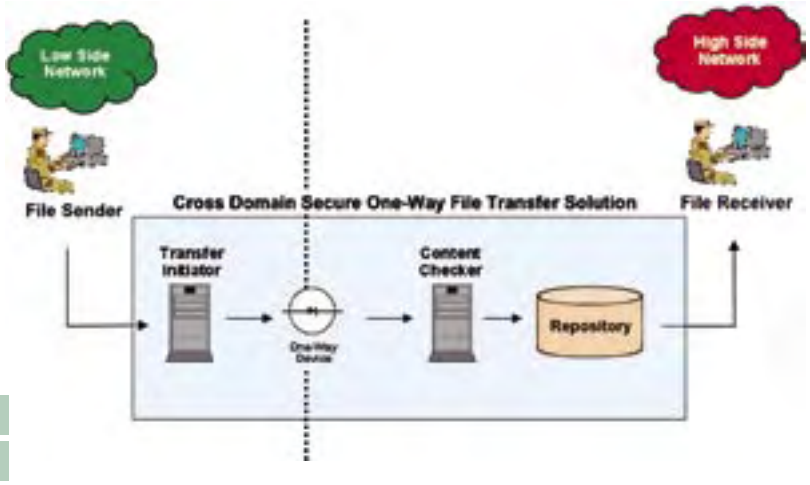
- MI2 successfully demonstrated seamless connection/interoperability of disparate chat utilities within and between state, local and federal agencies at all classification levels.
- MI2 successfully received, fused, and distributed data including weather data, air track from AMOC, SARS, Coast Guard GCCS, CAP alerts and graphical data, all in different data formats, enhancing situational awareness.
- MI2 successfully demonstrated the ability to act as a "middle-man" for data exchanges between the various systems, agencies, and networks and provided a capability to pass data from an unclassified network to the classified network without compromising security.

IT03.91
One Way File Transfer

3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: OneWay File Transfer (OWFiT) is a National Security Agency developed Cross Domain file transfer solution designed to mitigate the malicious code risk of introducing media and formatting rich files from a lower domain to a higher domain. The tool scans files for viruses and keeps infected files from transferring from an unclassified computer to a classified computer. OneWay File Transfer improves high-level capability categories of Multi-national Operations, Interagency Operations, and Command and Control.

SPONSOR: JSIC
TRIAL LOCATIONS:
NSWC Dahlgren, Hanscom AFB, USFK, NGA , AUS
TRIAL PARTNERS:
N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, OneWay File Transfer Interoperability Trial received a Warfighter, Interoperability, and Security assessment.

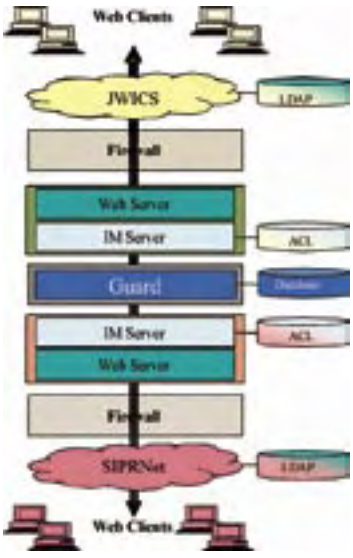
- OWFiT's ability to transfer files from an unclassified domain to a higher security domain while maintaining data integrity exhibited powerful potential to the military and coalition partners supporting mission objectives.
- OWFiT successfully demonstrated Multi-Level/Multi-Domain Protection by facilitating information sharing across multiple security information domains.
- OWFiT successfully detected Microsoft office and text files that had malicious code embedded within the file content and prevented transfer to a higher security domain.

IT03.92
Cross Domain CrossTalk

3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: Cross Domain CrossTalk provides text only instant messaging between authorized users on the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet). The tool allows instant messaging "chat" between users with a "need to know."

SPONSOR: CIA
TRIAL LOCATIONS:
NSWC Dahlgren, Hanscom AFB, USFK, NGA, AUS
TRIAL PARTNERS:
N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Cross Domain Cross Talk Interoperability Trial received a Warfighter, Interoperability, and Security assessment.

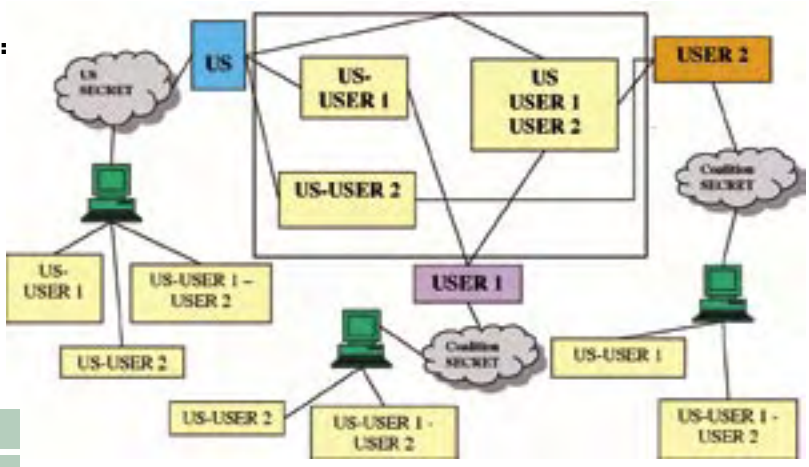
- Cross Domain Cross Talk successfully demonstrated Multi-Level/Multi-Domain Protection by facilitating information sharing across multiple information domains.
- Cross Domain Cross Talk successfully allowed multi-level collaboration via instant messaging between different security level domains.
- Cross Domain Cross Talk was limited in its ability to provide a means to facilitate information sharing across multiple information domains through the utilization of instant text messaging between secured and higher secured domains.

IT03.93
Multi-Level Chat

3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: Multi-Level Chat is a system that provides chat services on a multi-level secure (MLS) server. Multiple chat rooms operate at specific security levels and allow access based on user, network, clearances and permissions. The system provides filtering and monitoring services to chat room moderators who ensure releasable data is properly protected. The user interface is Web accessible or accessed from clients at existing national networks.

SPONSOR: JCIS
TRIAL LOCATIONS: NSWC Dahlgren, Hanscom AFB, USEUCOM, USFK, AUS
TRIAL PARTNERS: N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Multi-Level Chat Interoperability Trial received a Warfighter, Interoperability and Security assessment.

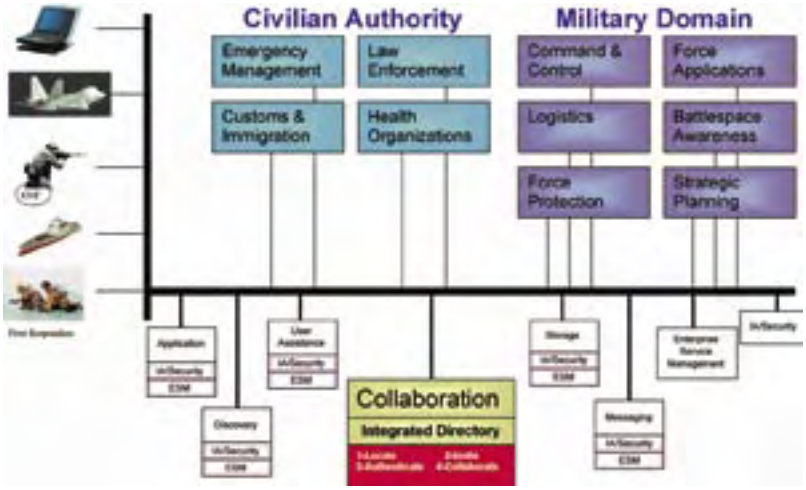
- Multi-Level Chat successfully demonstrated Multi-Level/Multi-Domain Protection by facilitating information sharing across multiple information domains.
- Multi-Level Chat successfully connected a MLS Chat server to networks of differing security levels. Multiple chat rooms created operated at specific levels and allowed access based on user, network clearances and permissions.
- Users observed Multi-Level Chat's ability to block and/or filter dirty words.

IT04.15
Integrated Directory/Collaboration Core Services

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: ID/C CS is a set of transformational core services and capabilities supporting cross-organizational communication, collaboration, and application interoperability. A web services accessible integrated directory and collaboration service support the ID/C CS capabilities. ID/C CS supports the creation of cross-organization teams of skilled individuals to address emerging problems, accommodate the information sharing policies and procedures of contributing organizations and automate directory discovery and integration. Users successfully search the integrated cross-organizational directory through the ID/C CS Collaboration Portal; perform e-mail, chat, e-meetings including whiteboard functions.

SPONSOR: OSD OFT
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, USEUCOM, USFK,NGA, AITS-JPO, AUS, CAN, UK, NATO
TRIAL PARTNERS: IT01.01, 01.85



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Integrated Directory/Collaboration Core Services Interoperability Trial received a Warfighter, Interoperability and Security assessment.

- ID/C CS successfully created and used the "Buddy List" function for collaboration
- ID/C CS demonstrated good collaborative functions for communicating and sharing information with specific users in a group environment, enhancing situational awareness and mission assurance.
- Overall the trial was successful and demonstrated solutions and offered techniques and procedures that enabled collaborative planning.

IT04.16
Instaknow Active Collaboration Engine

4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: Instaknow-ACE is a software platform that automates complex business processes. These processes interact with diverse applications, information sources and groups of people across the enterprise and with partners across the Internet on a real-time basis. Instaknow's uniqueness is that automation and integration is achieved by visually configuring solutions by Instaknow-ACE's "point & click" wizards. Program coding is not required and, in most cases, the customer's existing systems do not need modification to interface.

SPONSOR:
USNORTHCOM
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren,
SPAWAR
TRIAL PARTNERS:
N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Instaknow Active Collaboration Engine Interoperability Trial received a Warfighter and Interoperability assessment.

- Instaknow-ACE successfully demonstrated gathering data from multiple open data sources on the Internet, providing a composite picture for first responders.
- Instaknow-ACE successfully sent email and phone call notifications to users, enhancing situational awareness and providing collaborative planning across a bandwidth constrained operational environment.
- Instaknow-ACE proved to be a unique tool providing a viable solution to address requirements for database integration.
- The application demonstrated for CWID was created prior to execution, therefore Instaknow-ACE did not demonstrate the ability to create or change the application using the "point & click" wizards that are a key component of the system.

IT04.21
Collaborative Operational Planning System

1. MISSION ASSURANCE ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: Collaborative Operational Planning System (COPlanS) provides the ability to effectively plan, define courses of actions, and make operational decisions in a network centric environment with integrated collaborative tools. COPlanS supports planning team's processes and workflows enabling horizontal and vertical collaboration between planners. COPlan system provides the tools to review and replay decision paths for improving operational decision-making processes.

SPONSOR: Canada
TRIAL LOCATIONS:
Hanscom AFB,
USEUCOM, AUS,
CAN, NZ, UK, NATO
TRIAL PARTNERS:
N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Collaborative Operational Planning System Interoperability Trial received a Warfighter assessment and a SEIWG evaluation report.

- COPlanS successfully demonstrated the stated CWID objective by providing infrastructure that allowed a distributed planning team to collaborate on operational planning processes.
- COPlanS successfully provided a framework for flexible workflow processes allowing the distributed planning team to collaborate, both vertically and horizontally, in an organized and effective manner. Tasking orders were distributed through the email system for task delegation, and a chat tool aided with peer-to-peer collaboration.
- COPlanS provided a rich environment where planning information was entered and shared. Geospatial and time referenced (Gantt chart) data were supported.

IT04.26
Disaster Management Interoperability Services

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: DMIS is a "networked" directed distribution interoperability backbone (infrastructure). Directed distribution allows the sender to determine who receives the alert messages. DMIS consists of two elements - an Interoperability backbone and a suite of tools. DMIS successfully provided situational awareness by providing a network backbone that allowed participating trials and alert systems the ability to collaborate and pass written information about the incident efficiently and effectively across organizational boundaries. Trials using the DMIS Backbone share information between systems and facilitate a common operational picture for military and civilian users alike.

SPONSOR: FEMA
TRIAL LOCATIONS: NSWC Dahlgren
TRIAL PARTNERS: IT02.47, 02.58, 02.77, 03.70

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Disaster Management Interoperability Services Trial received an Interoperability assessment

- DMIS successfully demonstrated situational awareness by providing a "networked" directed distribution interoperability backbone that allowed other CWID trials and alert systems to send and receive Common Alerting Protocol (CAP) messages and in some cases incident response reports.
- All the trials and alert systems that participated in conjunction with the DMIS interoperability backbone successfully established a "network of infrastructures" by developing interfaces to/from each other per open interface specifications.
- DMIS enables different computer systems supporting disasters to talk to each other making military and civilian responders more efficient and effective, supporting mission assurance objectives.

IT04.31
Pathways to a National Cyber Security Response System

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: Pathways to a National Cyber Security Response System (PNCSRS) demonstrates capabilities of advanced network security technologies developed through government sponsored research and development efforts. PNCSRS provides network security management oversight of network attack sensing and warning, intrusion prevention, network security common operational picture, network security event visualization, and secure data communications. PNCSRS provides the ability to evaluate the impact of cyber attacks on government processes. PNCSRS provides crisis management support for threats or attacks on critical information systems, while coordinating with other agencies of the government to provide specific warning information and advice about appropriate protective measures and countermeasures.

SPONSOR: DHS
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT05.04

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Pathways to a National Cyber Security Response System Interoperability Trial received a Warfighter and Security Assessment and a SEIWG evaluation report.

- Successfully provided information assurance and cyber security to enable collaborative planning and promoted secure command mission assurance planning and execution.
- Established security information assurance policies and procedures and enhanced interoperability of information fusion while maintaining secure network operations.
- PNCSRS provided alert mechanisms supporting a national-level notification, coordination and mitigation effort for cyber-security operations.

IT04.32
Federated Collaboration Information Environment

4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: MS FCIE is a suite of Microsoft collaboration services selected to provide the Coalition classified network collaboration capabilities. MS FCIE is a combination of commercial collaboration technologies in a single warfighter console. Using existing software and Microsoft's portal technologies, MS FCIE provides chat, file sharing, military messaging and email collaboration services. The use of portal technologies merges document sharing, collaboration and workflow into a single command and control interface. MS FCIE's suite of tools uses Active Directory Federation Services to brokered secure access to shared coalition planning information across allied Active Directory Domains.

SPONSOR: Australia
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, AUS, CAN, UK
TRIAL PARTNERS: N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Microsoft Federated Collaboration Information Environment Interoperability Trial received a Warfighter, Interoperability and Security assessment.

- MS FCIE collaboration features demonstrated at US sites were file sharing (Sharepoint) and chat. MS. FCIE achieved marginal success as a collaboration tool at the US sites.
- MS FCIE collaboration tools at coalition sites achieved moderate success. The military messaging capability was sporadic.
- MS FCIE successfully demonstrated file sharing capabilities and "Communicator Chat" functionality; however, chat attachments would not always open.

IT04.54
Joint Air Mission Services

2. SITUATIONAL AWARENESS ● 3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ●

TRIAL OVERVIEW: Joint Air Mission Services is a net-centric information delivery system that allows web access to air mission data for air battle planning in the Coalition Air Operations Center for improved coalition interoperability. Access is based upon each coalition warfighters' nationality, rank, need to know and the domain in which they were operating and controlled using Security First Secure Parser, a secure cross-domain, multi-level security software solution technology. Common Access Cards (CAC), programmed with user access parameters, is used every network the warfighter accesses. Information the warfighter views can change depending on the security classification of the network accessed and user credentials.

SPONSOR: USAF
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, Hanscom AFB, USEUCOM, USFK, CAN, NATO
TRIAL PARTNERS: N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Joint Air Mission Services Interoperability Trial received a Warfighter, Interoperability and Security assessment.

- JAMS successfully demonstrated a multi-level secure web-based environment that provided access to TBMCS data information through a secure parser based on clearance levels, facilitating information sharing across multiple information domains and enhancing situational awareness.
- Due to a lack of CAC card resources JAMS did not demonstrate their full potential.

IT04.88
Incident Commanders' Radio Interface

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: The Incident Commanders' Radio Interface (ICRI) addresses the ability of first responders and public safety agencies to talk to each other during crises. ICRI is a physically small, light, rugged, rapidly deployable device to permit military and civilian first responders with incompatible radios to communicate across multiple RF spectra and telephone circuits. ICRI addresses the C2 interoperable communication issues of first responders by providing 2-5 public safety agencies with radio interoperability as any tactical situation unfolds. ICRI is a plug and play device and can be fully operational in less than five minutes. ICRI demonstrates the interoperability of dissimilar radios covering military, commercial, commercial telephones, cellular telephone, satellite links, Voice over Internet Protocol, and multiple voice communications platforms simultaneously.

SPONSOR:
USNORTHCOM
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren,
USEUCOM
TRIAL PARTNERS:
N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Incident Commanders' Radio Interface Interoperability Trial received a Warfighter assessment and a SEIWG evaluation report.

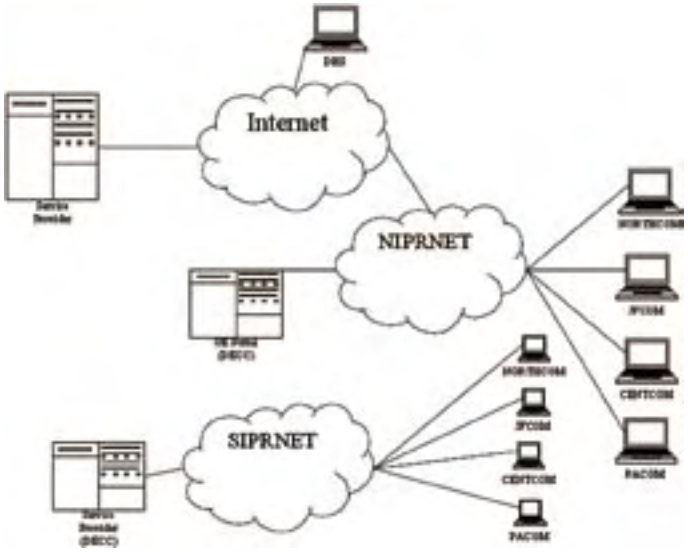
- Successfully provided a system that allowed first responders and responding agencies to communicate on a single system utilizing dissimilar radios and communication devices.
- Successfully demonstrated a collaborative information environment and received high reviews from users and visiting first responder agencies and counterparts. Cost-effective radio interoperability solution supporting both DoD and DHS.
- ICRI proved simple to deploy and required little training. It easily adapted to organizational changes at a first responder scene without technical support, operational at a first responder incident in less than ten minutes.

IT04.95
Next Generation Collaborative Services

4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: Next Generation Collaborative Services (NGCS), a web-based tool, provides a capability for virtual collaboration services (WebEx) supporting a net centric environment and facilitates communications and collaboration across organizations, agencies and jurisdictions in an unclassified environment. The system is a commercially managed tool offering collaborative functions for participants and does not require client software on individual PCs. NGCS allows users to share documents and applications, use whiteboards, perform text messaging and polling/voting, and use video and voice over IP. All these functions support a collaborative information environment for users, decision makers, and agencies.

SPONSOR:
USNORTHCOM
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren,
SPAWAR,
Hanscom AFB
TRIAL PARTNERS:
N/A



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Next Generation Collaborative Services Interoperability Trial received a Warfighter and Interoperability assessment.

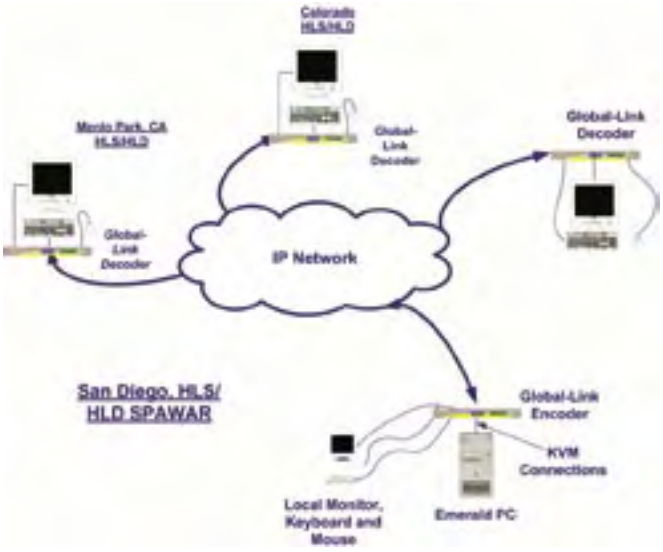
- NGCS successfully demonstrated the ability to provide collaboration services supporting a net centric environment using instant messages via chat and audio collaborations, whiteboarding, application sharing features for Word and Powerpoint documents, and polling and voting features via the Web.
- Due to bandwidth constraints, video functions were not demonstrated since Webcams were not used at any US site.
- NGCS successfully provided users situational awareness of Homeland Security/Homeland Defense issues, incidents and crisis events.

IT05.04
Global-Link

5. ISR DISSEMINATION ●

TRIAL OVERVIEW: Global-Link provides for the secure transmission of keyboard, high-resolution video, and mouse (KVM) using Internet Protocol (IP). Unlike other KVM over IP offerings, Global-link is a hardware solution that does not require any client/server software. Global-Link system consists of an encoder connected to the source computer and a local KVM console, and a decoder that connects to the user KVM display devices. Video signals are encrypted using 3DES and keyboard/mouse signals are encrypted using the secure socket shell (SSH). Unique algorithms maintain image integrity without the video artifacts associated with other KVM / IP solutions. There is no mouse latency (mouse trails) and only one mouse cursor on screen.

SPONSOR: US Navy
TRIAL LOCATIONS: SPAWAR
TRIAL PARTNERS: IT04.31



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Global-Link Interoperability Trial received a SEIWG evaluation report.

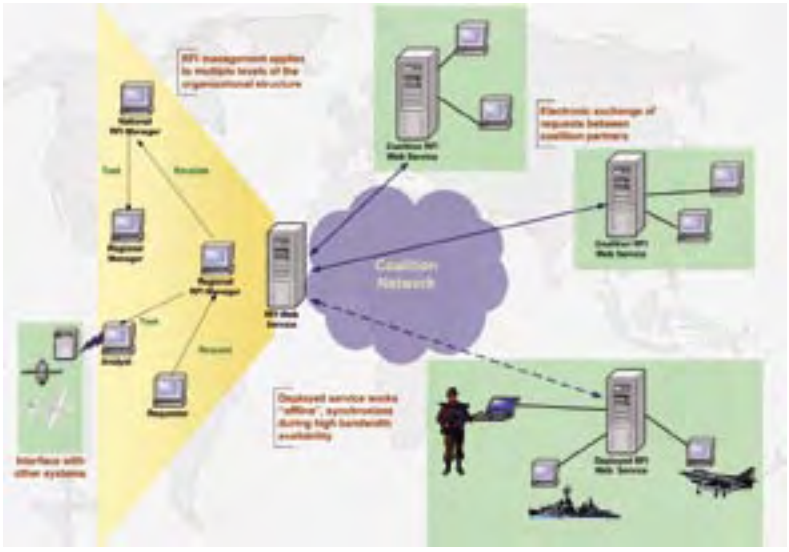
- Connected as a standalone system at SPAWAR to eliminate the network bandwidth issues on the CWID network, the Global-Link KVM product (decoder, keyboard, mouse and monitor) only supported the Coast Guard at San Diego Harbor; therefore, verification of trial operation could not be validated.
- Global-Link did not successfully demonstrate solutions to permit enhanced sharing and dissemination of intelligence, surveillance, and reconnaissance (ISR) products within and across information domains.

IT05.19
Request for Information Services Interoperability

1. MISSION ASSURANCE ● 2. SITUATIONAL AWARENESS ● 4. COLLABORATIVE INFORMATION ENVIRONMENT ●

TRIAL OVERVIEW: RFI SI is a single web site where all users converge to request geospatial information using thin-client technology. RFI SI demonstrates the capability to track and manage intelligence requests virtually, allowing for information sharing between organizations and nations. Users track the progress of the request through its lifecycle until an answer is offered. RFI SI provides a searching mechanism to filter out RFIs for action or review and is fundamental in providing timely intelligence information to commanders and decision makers. Request for Information Services Interoperability (RFI SI) is an enhancement to the current RFI system now used in Canada.

SPONSOR: Canada
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, USEUCOM, NGA, AUS, CAN, UK
TRIAL PARTNERS: IT02.08, 02.09, 02.30, 02.34, 02.42, 05.44



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Request for Information Services Interoperability Trial received a Warfighter assessment and a SEIWG evaluation report.

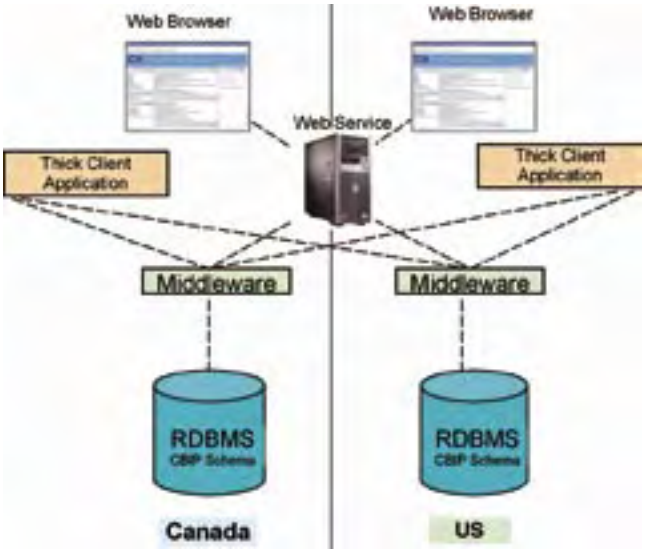
- RFI SI successfully managed intelligence requests within and between organizational and national boundaries. The RFI services tracked and managed intelligence requests virtually, allowing for information sharing between organizations and nations
- RFI SI successfully disseminated data from subject matter experts to users through a web-based environment.
- RFI SI successfully transferred requests electronically from one national system to another within the coalition operational environment.

IT05.24
Geospatial Intelligence Integration

5. ISR DISSEMINATION ●

TRIAL OVERVIEW: Geospatial Intelligence Integration (GII) presented a new concept of using two different databases at two different locations (Canada/US) for cross border incidents under the Homeland Defense scenario. The trial provides a unified cross border geospatial data set for national agencies at all levels with a common base infrastructure picture. Using Canadian geospatial data located on servers in Canada and US geospatial data from the National Geospatial Intelligence Agency (NGA) Image Product Library (IPL), GII fuses data from the two sources and produce a single accurate map of the border area. The Cross Border Infrastructure Plan (CBIP) tests the interoperability between Canada and US infrastructure data.

SPONSOR: Canada
TRIAL LOCATIONS: NGA, CAN
TRIAL PARTNERS: IT02.08, 02.09, 02.30, 05.19



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005 Geospatial Intelligence Integration Interoperability Trial received a Warfighter and Interoperability assessment.

- GII was partially successful in demonstrating a complete fused product of geospatial, imagery and infrastructure information for a cross-border situation.
- GII was successful in achieving visual fusion but only partially successful in achieving a common attribute schema. GII was not able to obtain geometric alignment and consequently it was not possible to use the fused product to conduct geospatial analysis.

IT05.44
Advanced Geospatial Imagery Library Enterprise

2. SITUATIONAL AWARENESS ● 5. ISR DISSEMINATION ●

TRIAL OVERVIEW: AGILE is a web-based technology suite of JPEG2000-compliant COTS software components enabling high performance access and visualization of large geospatial imagery in a dynamic manner. The AGILE server/client architecture enables fast compression, access to, and delivery of wavelet streaming imagery of the JPEG2000. Using wavelet compression technology, and AGILE's advanced visualization capabilities, users access and view large geospatial imagery for an identified region of interest faster than in the past, even with limited bandwidth. AGILE "extends the battlespace" by providing users, with less than ideal bandwidths, a better solution for imagery management.

SPONSOR: NGA
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, AUS, CAN, NZ, UK, NATO
TRIAL PARTNERS: IT02.42, 03.70, 05.19

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS
During CWID 2005, Advanced Geospatial Imagery Library Enterprise Interoperability Trial received a Warfighter and Interoperability assessment

- AGILE successfully demonstrated an enhanced situation awareness capability in a bandwidth constrained operational environment and provided dissemination of intelligence, surveillance, and reconnaissance (ISR) products within and across information domains.
- Users successfully used NGA IPL Quick Query to search for and retrieve imagery via metadata. Queries returned a link that allowed users to view the imagery as a JPEG2000 format with the AGILE client. AGILE provided a streaming capability vice downloading large files.
- AGILE provided a mechanism for performing mission tasks more quickly than in the past, improving warfighter productivity.

IT05.63

Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition

5. ISR DISSEMINATION ●

TRIAL OVERVIEW: In an operational environment, MAJIIC provides near real-time ISR data via a secure XML portal for forward deployed warfighters and can be interfaced with community publish/subscribe brokers. The MAJIIC system supports data dissemination and allows forces in remote locations to access information through web services as part of the Horizontal Fusion (HF) initiatives promoting data fusion. MAJIIC provides a single point for data access in common formatting, allowing information to flow to users in a timely fashion. MAJIIC facilitates expeditious dissemination of pre-tagged data based on users' access/permission levels.

SPONSOR:
USJFCOM
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren,
SPAWAR, USEUCOM
TRIAL PARTNERS:
N/A

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Multi-Sensor Aerospace-Ground Joint ISR Interoperability Trial received a Warfighter and Security assessment and a SEIWG evaluation report.

- MAJIIC successfully provided a solution for enhanced dissemination of ISR products within and across information domains or communities of interest.
- MAJIIC successfully demonstrated ISR data retrieval using web services and accessed ISR data by matching LDAP descriptions with information embedded in XML-tagged documents. Data provided to users was based on Role-based access control.

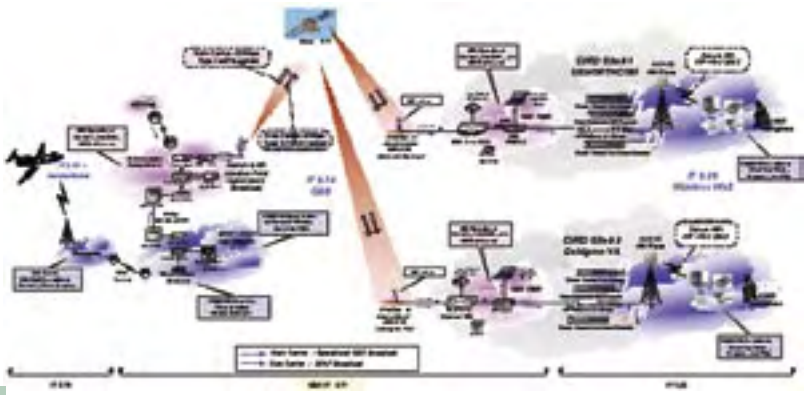
IT05.74

Posted Applications Over Return Channel Satellite

2. SITUATIONAL AWARENESS ● 3. MULTI-LEVEL/MULTI-DOMAIN PROTECTION ● 5. ISR DISSEMINATION ●

TRIAL OVERVIEW: Posted Applications Over Return Channel Satellite (PAORCS), or Global Broadcast Service (GBS), presents an enhanced architecture for real-time situational awareness and collaborative mission planning capabilities for deployed and dismounted warfighters operating in a Net-Centric Operations Warfare (NCOW) environment. The GBS downlink uses open-standards based on Digital Video Broadcast (DVB) technology, providing broadcast IP over satellite connection. GBS provides the warfighter a more comprehensive overview of the battlefield prior to engagement with a continuous, high data rate, one-way satellite broadcast capability able to support the simultaneous transmission and receipt of national and theater level generated information products to forces deployed, on the move (in transit), or in garrison.

SPONSOR: DISA
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren
TRIAL PARTNERS:
IT02.79, 06.25



COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Posted Applications Over Return Channel Satellite Interoperability Trial received a Warfighter and Security assessment and a SEIWG evaluation report.

- GBS successfully provided data products to tactical operations centers, and demonstrated the ability to integrate with wireless systems to further extend data to handheld equipment, such as a Portable Data Assistants (PDAs) held by a dismounted soldier.
- GBS successfully enhanced tactical situational awareness and enabled collaborative planning across a bandwidth constrained operational environment with wideband broadcasts of imagery, video (military and commercial), and data including intelligence, unmanned aerial vehicle (UAV) feeds, logistics data, maps, weather, and operational orders.
- GBS successfully validated using digital video broadcast-terrestrial (DVB-T) technology in a coalition SATCOM environment for providing enhanced intelligence, surveillance and reconnaissance dissemination to the warfighter using laptop computers.

IT06.25
WirelessWall

6. WIRELESS SECURITY ●

TRIAL OVERVIEW: WirelessWall is a software-only solution providing IPS 140-2 validated security for 802.11 WiFi and 802.16 WiMAX networks. WirelessWall turns COTS hardware into hardened appliances designed to provide information assurance for client-server and point-to-point applications. WirelessWall enhances interoperable situational awareness and improves ISR capabilities by enabling applications to communicate securely over wireless infrastructure. WirelessWall can be used to enable secure, timely information flow for dismounted warfighters by delivering data to wireless handheld and laptop computers. WirelessWall is currently deployed in locations throughout the U.S. government and industry, including providing secure wireless for more than 4,500 users at the U.S. Military Academy at West Point.

SPONSOR: DISA
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT02.42, 05.74

- Demonstration of transparent application access using FIPS 140-2 validated secure wireless communication
- Goals are to improve ISR and collaborative mission planning capabilities and increase situational awareness between geographically dispersed personnel and resources
- Applications include access to high-quality geospatial imagery (trial 2.42) and satellite-initiated delivery of Global Broadcast Services (GBS) video (trial 5.74)
- FIPS 140-2 validated Advanced Encryption Standard (AES) sensitive but unclassified (SBU) secure wireless link is provided by Cranite WirelessWall software running on COTS hardware (HP servers), using built-in Centrino or iPaq 802.11 wireless
- Long-range 802.11 coverage provided by Vivato extended range base stations, covering 3,000,000 square feet from a single phased array antenna panel; rogue access point detection provided by AirMagnet sensors

Secure wireless application access to data, video, and voice
Interoperability demonstrated with trials 2.42 and 5.74

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, WirelessWall Interoperability Trial received an Interoperability and Security assessment.

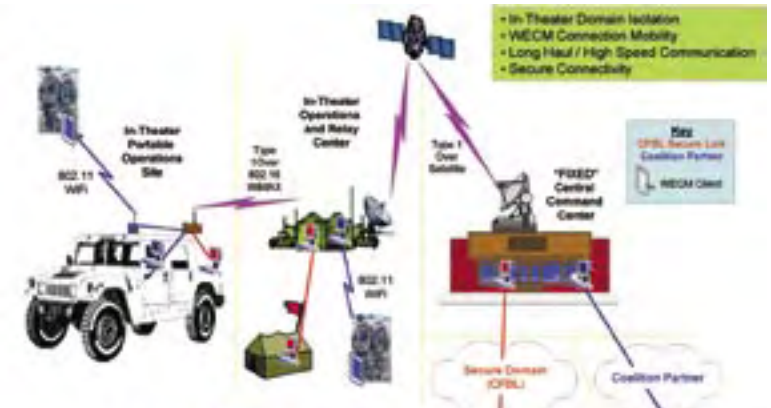
- WirelessWall network successfully provided a secure wireless link to disseminate mission assurance, situational assurance and ISR data to mobile devices in the field of operations.
- WirelessWall successfully provided a means to permit the transfer/receipt of the following types of data: .pdf, .wav, multicast traffic, and jpeg images over a secure wireless network.

IT06.37
Coalition Partner Mobile Command Center

6. WIRELESS SECURITY ●

TRIAL OVERVIEW: CPMCC is a dynamic coalition network and security solution that utilizes Network Centric Computing (NCC) technologies and Cryptek EAL 4-rated Virtual Private Network (VPN) devices to create a flexible and secure network-computing environment. CPMCC maintains and creates secure communities of interest across dynamic, mobile environments such as incident response and tactical operations. The solution includes secure, high performance satellite reach back to specific COI resources, and instant creation of a local incident response network over various LAN topologies including, 802.11, 802.16 and wired networks. The rapidly deployable secure network infrastructure supports locally and globally managed COIs and allows rapid recon figuration of the network(s) to support dynamically changing operational and political scenarios.

SPONSOR: USA RDECOM
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, USEUCOM
TRIAL PARTNERS: IT04.15



CRYPTEK Redline future technologies

COMPLETE REPORT
TRIAL CONTENTS
BOOKLET CONTENTS

ASSESSMENT RESULTS

During CWID 2005, Coalition Partner Mobile Command Center Interoperability Trial received a Warfighter, Interoperability and Security assessment.

- Utilizing the Cryptek and WECM hardware, CPMCC successfully demonstrated data exchange capabilities between fixed domains and mobile users and provided first responders and warfighters increased situational awareness through an encrypted wireless mechanism.
- Collaboration sessions that included chat, Bitmap graphical images, video, audio and document sharing were successfully demonstrated between wired and wireless role players. Security services were provided by Cryptek's EAL 4 Common Criteria evaluated (under NIAP) FIPS 140-2 Level 2 products but no formal events were conducted to test the impact of the security capabilities on interoperability.

Abbreviations and Acronyms

AAR ..... After Action Report
ACO..... Airspace Control Order
ADOCS..... Air Defense Operations Center System
AITS-JPO..... Advanced Information Technology Services - Joint Program Office
ATM ..... Asynchronous Transfer Mode
ASP ..... Application Service Provide; Active Server Page
ATO ..... Air Tasking Order
AWG ..... Assessment Working Group
Bi-SC ..... Bi (= two) Strategic Commands (ACE and ACLANT)
Bi-SC AIS ..... Bi-SC Automated Information System
C2..... Command and Control
C3..... Command, Control, Communications; Consultation, Command and Control
C4..... Command, Control, Communications, and Computers
C4I..... Command, Control, Communications, Computers and Intelligence
C4IFTW ..... C4I for the Warrior
CAOC ..... Combined Air Operations Center
CBRN ..... Chemical, Biological, Radiological, Nuclear
CCCC ..... Combined Communications Control Center
CCEB..... Combined Communications-Electronics Board
CCG..... Coalition Coordination Group
CCTF ..... Commander, Combined Task Force
CFACC ..... Coalition Force Air Component Commander
CFBLNet..... Combined Federated Battle Laboratories Network
CFLCC..... Coalition Force Land Component Commander
CFMCC..... Coalition Force Maritime Component Commander
CIAT..... Coalition Information Assurance Team
CITWG..... Coalition Interoperability Trials Working Group
CJCSI ..... Chairman of the Joint Chiefs of Staff Instruction
CJTF..... Combined Joint Task Force
COE..... Common Operating Environment
COI ..... Communities of Interest; Centers of Influence
COMSEC..... Communications Security
CONOPS..... Concept of Operations
COP..... Common Operational Picture
COTS..... Commercial-Off-The-Shelf
C/S/A ..... Combatant command, Services, and Agencies
CTF..... Combined Task Force
CVAT..... Coalition Vulnerability Analysis Team
CWAN..... Coalition Wide Area Network
CWID ..... Coalition Warrior Interoperability Demonstration
CWID JMO .... CWID Joint Management Office
DAA ..... Designated Approving Authority
DCIAI ..... Defense Capability Initiative Action Item
DCP..... Distributive Collaborative Planning
DCTS..... Defense Collaboration Tool Suite
DHS..... Department of Homeland Security
DII..... Defense Information Infrastructure
DISA ..... Defense Information Systems Agency
DISN-LES..... Defense Information Systems Network – Leading Edge Services
DMS..... Defense Message System
DoD ..... Department of Defense
DTRA..... Defense Threat Reduction Agency
FBI..... Federal Bureau of Investigation
FBO ..... Federal Business Opportunities
FEMA..... Federal Emergency Management Agency
FO..... Fiber-Optic
FPC ..... Final Planning Conference
FPGA..... Field Programmable Gate Array
GBS..... Global Broadcast System
GCCS ..... Global Command and Control System
GCSS ..... Global Combat Support System
GIG ..... Global Information Grid
GIS ..... Geographical Information System
GWOT ..... Global War on Terrorism
HF..... High Frequency
HLS ..... Homeland Security
HLD ..... Homeland Defense
HR ..... Humanitarian Relief
IA ..... Information Assurance
ICC..... Integrated Command and Control; Interim CAOC Capability
IER..... Interface Exchange Requirement
INFOSEC..... Information Security
IP ..... Internet Protocol
IPC..... Initial Planning Conference
IT ..... Interoperability Trial
JBC..... Joint Battle Command
JDCAT ..... JSIC Data Collection Analysis Tool
JITC..... Joint Interoperability Test Command
JSIC..... Joint Systems Integration Command
JTA..... Joint Technical Architecture
JTF ..... Joint Task Force
JWICS ..... Joint Worldwide Intelligence Communication System
JWID..... Joint Warrior Interoperability Demonstration (now CWID)
JWID JMO ..... JWID Joint Management Office (now CWID JMO)
Kbps ..... Kilo bits per second
LAN ..... Local Area Network
Mbps..... Mega bits per second
MCCIS..... Maritime Command and Control Information System
MISREP..... Mission Report
MLS ..... Multi-Level Security
MPC..... Mid-term Planning Conference
MSAB ..... Multinational Security Accreditation Board
MSEL..... Master Scenario Events List
MSL ..... Multiple Security Level
MTF ..... Multinational Task Force
MWBT..... MSEL Web-Based Tool
NACOSA..... NATO Communications and Information Systems Operating and Support Agency
NATO..... North Atlantic Treaty Organization
NC3A..... NATO Consultation Command and Control Agency
NC3O..... NATO Consultation Command and Control Organization
NIAP ..... National Information Assurance Partnership
NIAT..... National Information Assurance Team
NIETI ..... NATO Interoperability Environment Test Infrastructure
NIETWG..... NATO Interoperability Environment Test Working Group
NIPRNET..... Non-Secure Internet Protocol Router Network
NGA..... National Geospatial-Intelligence Agency
NOWG..... Network Operations Working Group
NSA ..... National Security Agency
O&M ..... Operations and Maintenance
OMIS ..... Operation Management Information System
OPORD ..... Operations Order
ORBAT ..... Order of Battle
PDA ..... Portable Data Assistants
PfP..... Partnership for Peace
PKO..... Peace Keeping Operation
PP ..... Participation Plan
PTE..... Prior to Execution
RDT&E ..... Research, Development, Test, and Evaluation
RFI..... Request for Information
RSGS ..... Regional Signal Group SHAPE
SBMC ..... Space Battle Management Center
SEIWG..... Systems Engineering and Integration Working Group
SEW ..... Shared Early Warning
SeWG..... Security Working Group
SHAPE ..... Supreme Headquarters Allied Powers Europe
SIPRNET..... SECRET Internet Protocol Router Network
SA..... Situational Awareness
SMG ..... Senior Management Group
SOP..... Standard Operating Procedure
SPAWAR ..... Space and Naval Warfare Systems Command
STDN..... Secure Tactical Data Network
TBMCS..... Theatre Ballistic Missile Control System
TBMD ..... Theatre Ballistic Missile Defense
TBONE ..... Theater Battle Operations Net-Centric Environment
TCP ..... Transformation Change Package; Transmission Control Protocol
TTP..... Tactics, Techniques and Procedures
USEUCOM .... United States European Command
USJFCOM ..... United States Joint Forces Command
USNORTHCOM...United States Northern Command
USPACOM..... United States Pacific Command
WAN ..... Wide Area Network
WAP..... Wireless Application Protocol
WARNORD.... Warning Order
WICAT ..... WISE Interoperability Collection and Management Tool
WISE ..... Web Information Services Environment
WSCI ..... Web Services for Coalition Interoperability

UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS

LOOK FORWARD

Objectives for CWID 2006

COALITION COMMAND AND CONTROL (C2)

- Enhance the Commander's Coalition C2 capability through secure, scalable and bandwidth sensitive technologies, within and between communities of interest (COIs) and information domains of differing security classifications.
  - Create a cohesive C2 relationship with and between military, coalition and non-military activities
  - Improve open and secure mobile C2 capabilities between COIs
  - Streamline operational decision-making for Global War on Terrorism (GWOT) contingencies

EXPLANATION: Coalition operations require an information environment that spans multiple COIs. These COIs may be mobile, fixed or remotely located where the combination of military and/or civil agencies is likely to be affected by limited bandwidth. Within any COI, mission success relates to the commander's C2 ability to communicate directly with individual users who may be detached from fixed information domains. Decision makers and/or first responders require interoperable, reliable and/or secure wireless capabilities to receive and transmit critical voice, data, and video information to support the Network Centric warfare construct.

COALITION INFORMATION SHARING

- Provide solutions that improve the Commander's ability to share information within a multi-lingual coalition that is secure, scalable and bandwidth sensitive. Included in this objective are improvements to language translation tools that provide grammatically correct, militarily appropriate context, multi-language translations to support verbal and textual collaboration within and between disparate information domains.
  - Multi-level and multi-domain security
  - Improve utility, accuracy and language capacity of translation tools
  - Written-to-voice, visa versa
  - Voice-to-voice
  - User friendly displays

EXPLANATION: Coalition information sharing is more than providing a common operational picture at the strategic or major echelon level of command. It must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare. Trial proposals should be capable of using existing interface standards and protocols that define the format, content, and exchange mechanisms for shared data. Solutions must support each nation's disclosure and release policies as well as provide a secure means of consistently communicating accurate information in a multi-lingual military and/or local authority context. Possible information to exchange includes: directive commentary, friendly and hostile order of battle, targeting information, safe areas for marshalling, weather data, imagery, Global Information Services (GIS) map data, equipment status, personnel movements and other intelligence related products. A key subset to creating and sustaining a coalition information sharing environment is that users must be able to consistently and securely access, extract and utilize common information derived from dissimilar databases across multiple domains.

INTEGRATED LOGISTICS

- Provide solutions for responsive, effective logistics within and between multiple information COIs.
  - Develop the ability to assess and display information on the movement, location and status of U.S. and coalition partners' equipment and personnel en route and/or deployed
  - Improve logistics data access, fusion and integration among COIs

EXPLANATION: Within the information environment of a coalition, military and non-military operations, the commander must have responsive and effective logistics. Logistic data is contained within diverse logistics information systems maintained by military and civilian agencies across the coalition. Access to that data implies combining total asset visibility and information during the transit of friendly forces into a single information presentation available across multiple information COIs.

CONTINUITY OF OPERATIONS

- Provide C2 solutions that enhance the Commander's ability to plan, communicate and affect coalition operations while remotely deployed. Inherent in this objective is the ability of the commander to maintain situational awareness and connectivity with subordinate activities while en route to the theater in crisis.
  - Enhance Commander's ability to rapidly deploy a joint force headquarters

EXPLANATION: Commanders are challenged to sustain their situational awareness once they depart on their assigned mission. Trial proposals must be capable of using existing interface standards and protocols that define the format, content, and exchange mechanisms for shared data. Possible information requirements include: friendly and hostile order of battle, targeting information, safe areas for marshalling, weather data, imagery, GIS map data, equipment status, personnel movements and other intelligence-related information. When appropriate, the solution must be scaleable to provide GIS and GCCS situational awareness information to non-military, federal, state and local participants via a protected, multi-lingual and secure network, common to all. Information exchange should support pre-event and en route planning as well as situational awareness during the execution of operations.

NET CENTRIC ENTERPRISE SERVICES

- Provide solutions that enhance the Commander's ability to collaborate and disseminate information among COIs in a Net Centric environment.
  - improve information assurance
  - improve horizontal data access, fusion and integration
  - improve vertical and horizontal information distribution

EXPLANATION: Network Centric Enterprise Services imply that coalition, military and non-military civilian authorities can harness the power of their respective information environments to collaboratively plan and execute operations even in a bandwidth-constrained environment. Collaborative planning and dissemination of products in a bandwidth constrained environment horizontally across and vertically within COIs is an emerging issue for the warfighter, particularly as software and procedure tools become sufficiently robust to be extended from the operational to the tactical level of warfare. Operations require an information environment that is not only scaleable, but one that spans multiple COIs. These COIs may be populated and maintained by military or civil agencies or a combination of both, likely bandwidth-constrained. The information exchange between these COIs must be accomplished so that it inspires confidence at each activity that the information is being disseminated, and only available to agreed upon and authorized participants.

USEUCOM is host Combatant Commander for CWID 2006 and 2007. Definition of objectives initiated the trial submission process in 2005 through publication to Federal Business Opportunities: www.fedbizopps.gov

KEY DIFFERENCES FOR 2006

1. Number of objectives reduced to narrow focus of CWID and reflect the recurring theme "Coalition Information Sharing"

2. Each objective is supported by sub-objectives that reference clearly defined U.S. Combatant Commander and Coalition capability gaps

3. Each sub-objective is related to the U.S. Universal Joint Task List to link warfighter mission-to-task requirements

UNABRIDGED REPORT
BOOKLET CONTENTS
TRIAL CONTENTS
ACRONYMS